HIRSCHMANN

A BELDEN BRAND

Reference Manual

GUI Graphical User Interface
EAGLE20/30

RM GUI EAGLE20/30
Release 1.0 10/2012

Technical Support
https://hirschmann-support.belden.eu.com

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

Rel. 1.0 - 10/2012 – 11.10.12

Contents

About this Manual

The “GUI” reference manual contains detailed information on using the graphical interface to operate the individual functions of the device.

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Basic Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The Industrial HiVision Network Management Software provides you with additional options for smooth configuration and monitoring:

- Simultaneous configuration of multiple devices
- Graphic interface with network layout
- Auto-topology discovery
- Event log
- Event handling
- Client/server structure
- Browser interface
- ActiveX control for SCADA integration
- SNMP/OPC gateway.

Key

The designations used in this manual have the following meanings:

▶	List
□	Work step
■	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in user interface

Graphic User Interface (Web-based Interface)

■ System requirements

To open the graphical user interface, you need a Web browser, for example Mozilla Firefox version 3.5 or later, or Microsoft Internet Explorer version 6 or later.

■ Installation

Note: The graphical user interface uses Java 6 or Java 7.

Install the software from the enclosed CD-ROM. To do this, you go to “Additional Software”, select `Java Runtime Environment` and click on “Installation”.

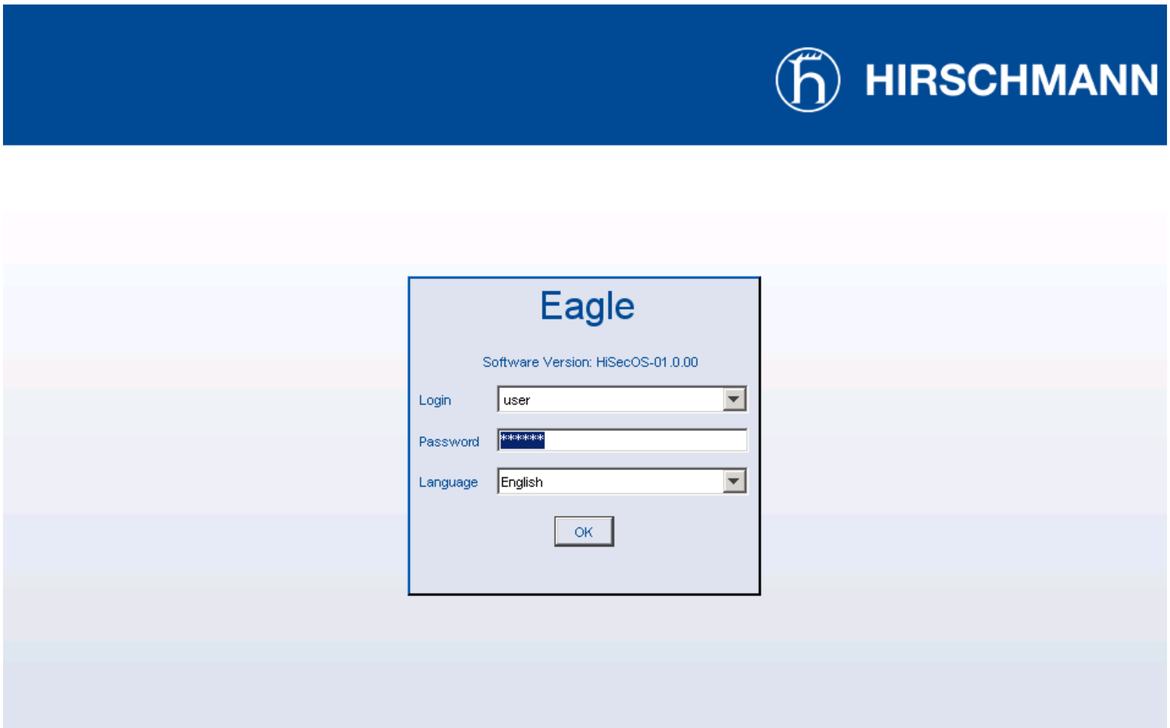
■ Starting the graphic user interface

The prerequisite for starting the graphical user interface, first configure the IP parameters of the device correctly. The “Basic Configuration” user manual contains detailed information that you need to define the IP parameters.

□ Start your Web browser.
□ Activate Java in the security settings of your Web browser.
□ Establish the connection by entering the IP address of the device which you want to administer via the Web-based management in the address field of the Web browser. Enter the address in the following form:

```
https://xxx.xxx.xxx.xxx
```

The login window appears on the screen.



Eagle

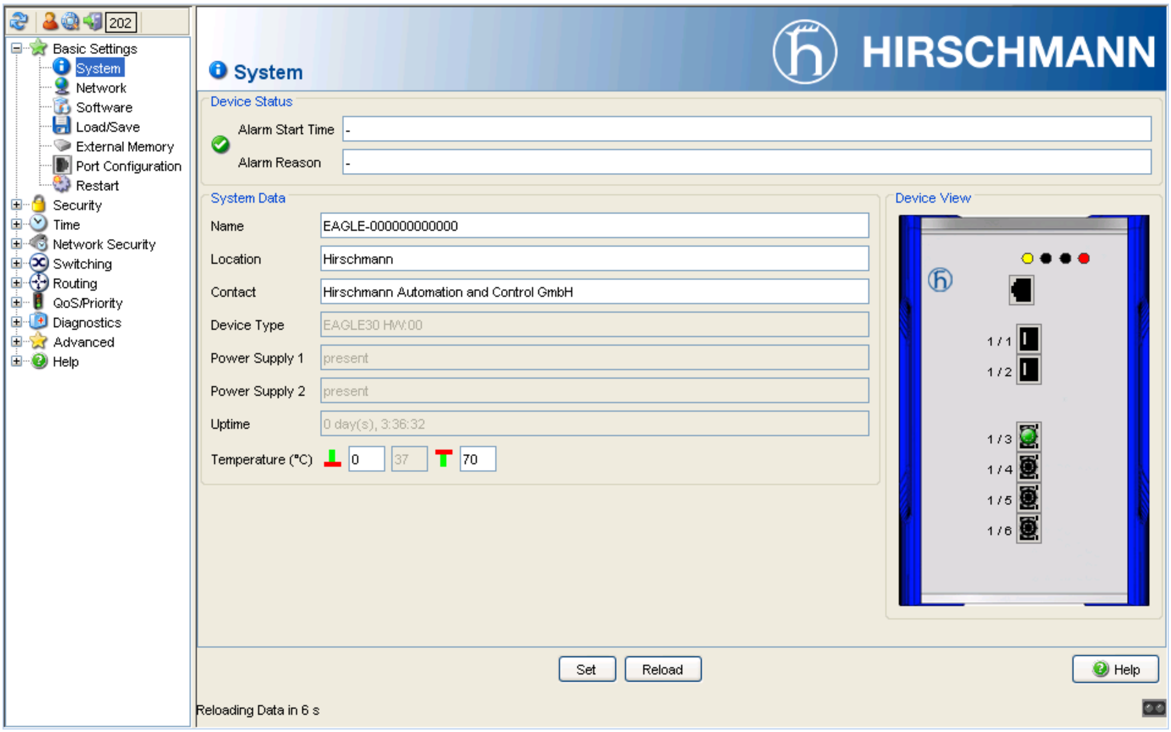
Software Version: HiSecOS-01.0.00

Login: user
Password: ******
Language: English

Figure 1: Login window

□ Select the user name and enter the password.
□ Select the language in which you want to use the graphic user interface.
□ Click on OK.

The window with the graphic user interface will appear on the screen.



System

Device Status

Alarm Start Time: -

Alarm Reason: -

System Data

Name: EAGLE-000000000000

Location: Hirschmann

Contact: Hirschmann Automation and Control GmbH

Device Type: EAGLE30 HW:00

Power Supply 1: present

Power Supply 2: present

Uptime: 0 day(s), 3:36:32

Temperature (°C): 0 37 70

Device View

Reloading Data in 6 s

Figure 2: Graphic user interface of the device

Operating Instructions

The graphical user interface of the device is divided into the menu part (left) and the dialog part (right).

The menu shows the menu items. You click on a menu item to display the corresponding dialog in the dialog part.

You right-click in the menu part to open the context menu:

- You use "Back" to go back to any menu item you previously selected.
- You use "Forward" to go forward to any menu item you previously selected.

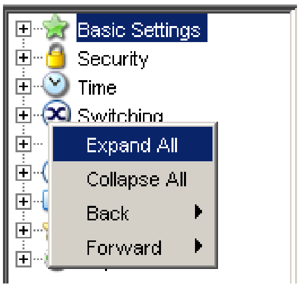


Figure 3: Menu with context menu

The tool bar is located above the menu.

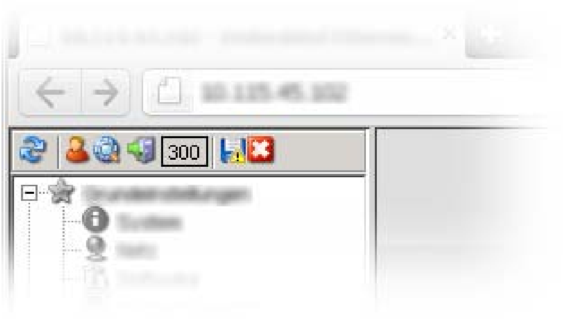


Figure 4: Tool bar

The tool bar contains the following buttons:

Button	Function
🔄	Refreshes the display in the tool bar with the values from the volatile memory (`RAM`) of the device.
❌	Terminates the refreshing of the display.
👤	When you position the mouse pointer over the button, a bubble help appears with the following information: ▶ Name of the user logged on ▶ Device name ▶ Network protocol of the connection between the graphical user interface and the device By right-clicking this symbol you can open the `Basic Settings:System` dialog and the `Basic Settings:Network` dialog directly.
🔍	When you position the mouse pointer over the button, a bubble help appears with the summary of the `Diagnostics:Configuration Check` dialog. By right-clicking this symbol you can open the `Diagnostics:Configuration Check` dialog directly.
🚪	Ends the session for the logged on user (logout).
297	Shows the period of inactivity in seconds after which the device ends the session for the logged on user. You specify the timeout period for the session in the `Security:Management Access:Web` dialog.
💾	Shows that the device configurations in the volatile memory (`RAM`) and the non-volatile memory (`NVM`) are different. By right-clicking this symbol you can open the `Basic Settings:Load/Save` dialog directly. To refresh the display after changing the device configuration, click the button 🔄. To permanently save the changes, choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".

Table 1: Buttons in the tool bar

Button	Function
☒	When you position the mouse pointer over the button, a bubble help appears with information on the starting time and cause of the current alarm, as well as the settings of the boot parameters: ▶ Under "Device Status" you will find a summary of the messages from the "Device Status" frame in the `Basic Settings:System` dialog. ▶ Under "Boot Parameters" you will find a note if you permanently save changes to the device configuration and at least one boot parameter differs from the device configuration used during the last restart. The following settings cause the boot parameters to change. – The "Port Number" parameter in the `Security:Management Access:Server` dialog, "SNMP" tab – The "Activate SysMon1" parameter in the `Diagnostics:Selftest` dialog. – The "Load default config on error" parameter in the `Diagnostics:Selftest` dialog.

Table 1: Buttons in the tool bar (Cont.)

Instructions for saving the device configuration

□ To copy changed settings to the volatile memory (`RAM`), click the "Set" button.
□ To refresh the display in the dialogs, click the "Reload" button
□ To keep the changed settings even after restarting the device, click the `Save` button in the "Basic Settings:Load/Save" dialog.

Note: Unintentional changes to the device configuration may cause the connection between your PC and the device to be terminated. Before you change the settings in the device, switch on the function "Undo Modifications of Configuration" in the `Basic Settings:Load/Save` dialog. With this function, the device restores the active device configuration saved in the NVM if the connection is interrupted after the settings have been changed. The device remains reachable.

1 Basic Settings

With this menu you can configure the basic settings of the device.

The menu contains the following dialogs:

- System
- Network
- Software
- Load/Save
- External Memory
- Port Configuration
- Restart

1.1 System

With this dialog you can display and monitor the following properties of your device:

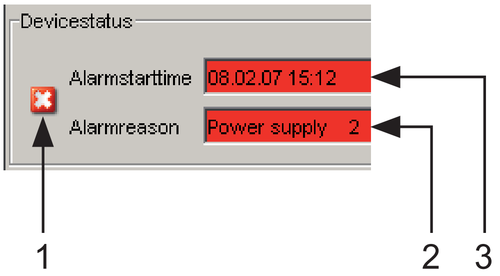
- Device status (time and cause of an alarm)
- System data (status of the power supply, operating time of the device)
- Device view (view of device with display elements, interfaces, device ports and their properties)

In this dialog you enter the following settings:

- Device name
- Location of device
- Contact person for device
- Temperature thresholds for the device

Device Status

This area of the graphical user interface provides information on the device status and the alarm state of the device.



Devicestatus

Alarmstarttime 08.02.07 15:12

Alarmreason Power supply 2

Figure 5: Device status and alarm display
1 - Device status symbol
2 - Alarm reason
3 - Alarm time

Designation	Meaning	Possible values
Device status symbol	Shows the device status.	✓ Device status OK ✖ Alarm occurring
Alarm Start Time	Start of the oldest existing alarm in format Month Day, Year hh:mm:ss AM/PM.	
Alarm Reason	Cause of the oldest existing alarm.	

Table 2: Device status and alarm display

Note: If you only select one power supply, the device detects the missing second power supply as an error. To avoid this error message, switch off the monitoring of the missing second power supply in the `Diagnostics:Device Status` menu.

System Data

This area of the graphical user interface displays the system parameters of the device. In the fields with a white background, you have the option of changing the settings.

Designation	Meaning
Name	Defines the device name. Possible values: ▶ 0..255 alphanumeric characters
Location	Defines the location of the device. Possible values: ▶ 0..255 alphanumeric characters
Contact	Defines the contact person for this device. Possible values: ▶ 0..255 alphanumeric characters
Device Type	Shows the product name of the device or, for modular devices, the product name of the basic device.
Power Supply P1	Displays the status of power supply P1. Possible values: ▶ `Present` ▶ `Not present` ▶ `Defective`
Power Supply P2	Displays the status of power supply P2. Possible values: ▶ `Present` ▶ `Not present` ▶ `Defective`
Uptime	Shows the time that has elapsed since this device was last restarted. Possible values: ▶ `day(s), hh:mm:ss`
Temperature (°C)	– Device temperature: Shows the current temperature in the device. – Temperature thresholds: Defines the lower/upper temperature threshold values. If the temperature goes outside this range, the device generates an alarm. Possible values: ▶ `-99..99` (integer) The “Installation” user manual contains detailed information about setting the temperature thresholds.

Table 3: System Data

Device View

The device view shows the front of the device.

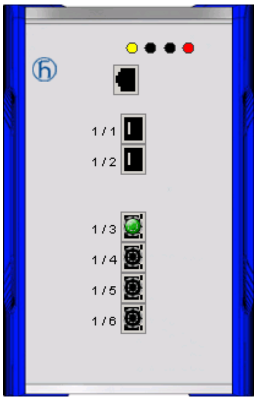


Figure 6: Device View

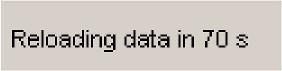
The following symbols represent the status of the individual device ports. In some situations, some of these symbols interfere with one another. You get a full description of the port status when you position the mouse pointer over the port symbol.

Criterion	Symbol	
Bandwidth of the device port	•	10 Mbit/s Port activated, connection okay, full-duplex mode
	●	100 Mbit/s Port activated, connection okay, full-duplex mode
	⬤	1000 Mbit/s Port activated, connection okay, full-duplex mode
Operating state	⦶	Half-duplex mode activated See the `Basic Settings:Port Configuration` dialog, "Automatic Configuration" checkbox.
	◎	Autonegotiation activated See the `Basic Settings:Port Configuration` dialog, "Automatic Configuration" checkbox.
AdminLink	⊖	Port is deactivated, connection okay
	⊖	Port is deactivated, no connection set up See `Basic Settings:Port Configuration` dialog, "Port on" checkbox and "Link/Current Settings" field.

Table 4: Symbols identifying the status of the device ports

Reloading

This area of the graphical user interface at the bottom left displays the countdown time until the applet requests the current data of this dialog again. Clicking the “Reload” button immediately calls up the current data for the dialog. The applet polls the current data of the device automatically every 100 seconds.



Reloading data in 70 s

Figure 7: Time to next Reload

Note: The device only periodically updates the `System` menu automatically.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 5: Buttons

1.2 Network

This dialog allows you to define the basic settings for accessing the management functions of the device via the network.

You define the following settings in the device:

- IP parameters
- VLAN ID
- Parameter for access via the HiDiscovery software
  The HiDiscovery software shows all the devices that can be reached in the network and allows you to configure their IP parameters.

■ Information

Parameters	Meaning
MAC Address	Displays the MAC address of the device.

Table 6: "Network" dialog, "Information" frame

■ Local

Parameters	Meaning
IP Address	Defines the IP address under which the management functions of the device can be reached. Possible values: ▶ Valid IPv4 address ▶ Default setting: —
Netmask	Identifies the network prefix of the network and the host address of the device in the IP address. Possible values: ▶ Valid IPv4 netmask ▶ Default setting: —
Gateway Address	Defines the IP address of the router via which the device reaches other devices outside its own network. Possible values: ▶ Valid IPv4 address ▶ Default setting: —

Table 7: "Network" dialog, "Local" frame

■ VLAN

Parameters	Meaning
ID	Defines the ID of the VLAN in which the management functions of the device can be reached. You can only access the management functions via the device ports that are members of this VLAN. Possible values: ▶ `1..4042` (default value: `1`)

Table 8: "Network" dialog, "VLAN" frame

■ HiDiscovery protocol

Parameters	Meaning
Operation	Activate the function to use the HiDiscovery software to assign the IP parameters to the device from your PC. Possible values: ▶ `On` (default value) ▶ `Off`
Access	With the HiDiscovery software you can also access the device if it does not have any IP parameters yet: ▶ `readWrite` (default value) This setting allows you to change the IP parameters of the device using the HiDiscovery software. ▶ `readOnly` This setting allows you to view the IP parameters of the device using the HiDiscovery software. The IP parameters are write-protected. Recommendation: Only change the setting to `readOnly` after putting the device into operation.

Table 9: "Network" dialog, "HiDiscovery Protocol" frame

Note: The HiDiscovery software only accesses the device via device ports on which routing is switched off and which are assigned to the same VLAN as the management of the device.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 10: Buttons

1.3 Software

With this dialog you can display information about the device software and update the device software.
You also have the option to restore a backup of the device software.

■ Version

Parameters	Meaning
Stored Version	Show the version of the device software stored in the flash memory. The device loads this software when it restarts.
Running Version	Shows the version of the device software currently running.
Backup Version	Shows the version of the device software stored in the flash memory that the device ran before the last software update.
Restore	Switches the "Stored Version" and the "Backup Version" of the device software, as well as the related device configurations. To load the restored device software, restart the device.
Bootcode	Shows the version of the bootcode software.

Table 11: "Software" dialog, "Version" frame

■ Software Update

Parameters	Meaning
File	Defines the path and the file name of the software image with which you update the device software. The device provides you with the following options for the software update: ▶ File upload If the software image is on your PC or on a network drive, click " … " and select the file with the ending `*.bin` there. ▶ SFTP or SCP upload The device allows you to transfer the software image from your PC to the device using SFTP or SCP: □ On your PC, open an SFTP or SCP client, e.g. WinSCP. □ Use the SFTP or SCP client to open a connection to the device. □ Transfer the file with the ending `*.bin` to the directory `/upload/firmware` on the device. When the file is completely transferred, the device starts updating the device software. If the update was successful, the device creates an `ok` file in directory `/upload/firmware` and deletes the file with the ending `*.bin`. □ To load the updated device software, restart the device.
…	Shows the "Open" dialog. You select the software image here if the file is located on your PC or on a network drive.
Update	Updates the device software with the software image specified in the "File" field. To load the updated device software, restart the device.

Table 12: "Software" dialog, "Software Update" frame

Table

Parameters	Meaning
File Location	Shows the storage location of the software image. Possible values: ▶ RAM Volatile memory of the device ▶ FLASH Non-volatile memory (NVM) of the device ▶ SD CARD External memory SD card (ACA31) ▶ USB External memory USB stick (ACA21)
Index	Shows the index of the software image. For the software images in the flash memory, the index has the following meaning: ▶ 1 The device loads this software image when it restarts. ▶ 2 This software image is a backup of the software that the device ran before the last software update.
File name	Shows the device-internal file name of the software image.
Firmware	Shows the version number of the software image and the time it was created.
Applet	Shows the version number of the graphical user interface (GUI) contained in the software image.

Table 13: "Software" dialog, table

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 14: Buttons

1.4 Load/Save

During operation, the device stores changed settings in the volatile memory (RAM) when you click "Set" in one of the dialogs. This dialog allows you to save the settings for the device permanently.

In the non-volatile memory you manage up to 20 different device configurations. You can save the device configurations encrypted or unencrypted on the PC or on an FTP server, or copy them from there.

Unintentional changes to the device configuration may cause the connection between your PC and the device to be terminated. Before you change the settings in the device, switch on the function "Undo Modifications of Configuration". With this function, the device restores the active device configuration saved in the NVM if the connection is interrupted after the settings have been changed. The device remains reachable.

■ External Memory

Parameters	Meaning
Active ENVM	Defines the active external memory. Possible values: ▶ SD The SD memory card (ACA31) is the active external memory. ▶ USB The USB stick (ACA21) is the active external memory. The device saves the device configuration on the active external memory. **Note:** The "Status" field in the Basic Settings:External Memory dialog shows the operating state of the connected external memory.

Table 15: "Load/Save" dialog, "External Memory" frame

Configuration encryption

Parameters	Meaning
Active	Shows whether the device configuration is encrypted and there is a password to make unauthorized access more difficult. Possible values: ▶ `not selected` The device configuration is unencrypted and can be read without a password. ▶ `selected` The device configuration is encrypted and has a password.
Set Password	Displays the "Set Password" dialog. Enter a new password and, if applicable, the existing password. ▶ The device encrypts the device configuration and uses a password to make unauthorized access more difficult. ▶ The device only accepts another device configuration during activation if the password used there matches the password set. ▶ Before replacing a defective device, prepare the new device as follows, if the device loads the device configuration from the external memory (`ENVM`) during a restart: □ Start the new device with the standard device configuration (`default configuration`). □ Enter the currently used password in the new device. □ Install the active external memory of the defective device in the new device. □ In the table, select the device configuration located on the external memory (`ENVM`). □ Click "Activate" to transfer the device configuration to the volatile memory (`RAM`). The device immediately uses this device configuration in the current operation.
Delete	Shows the "Delete" dialog. Enter the currently used password to neutralize the password protection.

Table 16: "Load/Save" dialog, "Configuration Encryption" frame

Information

Parameters	Meaning
NVM synchron to running config	Shows whether the device configurations stored in the volatile and non-volatile memories differ. Possible values: ▶ `Selected` The device configurations in the volatile memory (`RAM`) and in the non-volatile memory (`NVM`) are synchronized. ▶ `Not selected` The device configurations in the volatile memory (`RAM`) and in the non-volatile memory (`NVM`) are different.
ENVM synchron to NVM	Shows whether the currently active device configuration in the external memory (`ENVM`) is synchronized to the active device configuration in the non-volatile memory (`NVM`). Possible values: ▶ `Selected` The device configuration in the external memory (`ENVM`) is synchronized to the device configuration in the non-volatile memory (`NVM`). ▶ `Not selected` The device configuration in the external memory (`ENVM`) is different from the device configuration in the non-volatile memory (`NVM`).

Table 17: "Load/Save" dialog, "Information" frame

■ Undo Modifications of Configuration

Parameters	Meaning
Function	When a user switches on the function, the device checks whether it can still be reached from the IP address of the user. If the connection to this IP address is interrupted after the device configuration is changed, the device restores the active device configuration saved in the NVM. Save the current device configuration permanently before switching on the function. Possible values: ▶ `On` Function is switched on: – When you switch on the function, the device checks whether it can still access your PC via the network. – If the device is not accessible for longer than is specified in the field "Period to undo while Connection is lost [s]", it restores the active device configuration saved in the NVM. ▶ `Off` (default setting) Function is switched off. Switch the function off again after you have successfully changed the device configuration. You thus prevent the device from restoring the last permanently saved device configuration after the graphical user interface is closed.
Period to undo while Connection is lost [s]	Specifies the time in seconds after which the device restores the last device configuration saved if the connection to the device is interrupted after the device configuration is changed. Possible values: ▶ `30..600` (default setting: `600`) Specify a sufficiently large value. Take into account the time when you are only viewing the dialogs of the graphical user interface without changing or updating them.
Watchdog IP Address	Shows the IP address of the PC on which you have activated the function. Possible values: ▶ IPv4 address (default setting: `0.0.0.0`)

Table 18: "Load/Save" dialog, "Undo Modifications of Configuration" frame

■ Table

Parameters	Meaning
Storage Type	Shows the storage location of the device configuration. Possible values: ▶ RAM (volatile memory of the device) The volatile memory stores the device configuration that the device uses in the current operation. ▶ NVM (non-volatile memory of the device) In the non-volatile memory you store multiple device configurations. If you select a table entry and click "Activate", you load this device configuration to the volatile memory (RAM) of the device. ▶ ENVM (external memory) On the external memory the device saves backup copies of the device configurations that are located in the non-volatile memory - see the Basic Settings:External Memory dialog.
Name	Shows the name of the saved device configuration. If you select a table entry and click "Save As…", you can specify the name of the device configuration.
Modification Date	Shows the time at which a user last changed the settings of the device in the device configuration.
Active	Shows the active device configuration. Possible values: ▶ Selected The table entry contains the active device configuration. – The device loads the device configuration into the volatile memory (RAM) during the next restart. – When you click "Save", the device saves the settings permanently in this device configuration. ▶ Not selected The table entry does not contain an active device configuration. To specify the active device configuration, select a table entry and click "Select".

Table 19: "Load/Save" dialog, table

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Save	Transfers the saved device configuration from the volatile memory (`RAM`) to the non-volatile memory (`NVM`). The aim is the active device configuration, whereby the checkbox in the "Active" column is `selected`.
Activate	Transfers the device configuration of the selected table entry from the non-volatile memory (`NVM`) to the volatile memory (`RAM`). ▶ The device immediately uses this device configuration in the current operation. ▶ In the "Active" column, the checkbox is now `selected`. The device closes the connection to the graphical user interface. □ Reload the graphical user interface. □ Login again. You can only activate the device configuration if the password used matches the password set in the "Configuration Encryption" frame. Switch on the function "Undo Modifications of Configuration" before you activate a device configuration. With this setting the device activates the previous device configuration after the set time has elapsed, if the connection is interrupted after the device configuration is changed. The device can then be accessed again.
Delete	Removes the selected table entry. Prerequisite: The table entry does not contain an active device configuration - the checkbox in the "Active" column is `not selected`.
Select	Defines the selected table entry as the active device configuration: ▶ In the "Active" column, the checkbox is now `selected`. ▶ The device loads the device configuration into the volatile memory (`RAM`) during the next restart. ▶ The device saves the settings permanently in this device configuration when you click "Save". The device accepts the device configuration during the next restart only if the password used matches the password set in the "Configuration Encryption" frame. Otherwise no readable device configuration is available for the device when it is restarting. In the `Diagnostics:Selftest` dialog, you define whether in this case the device starts with the standard device configuration (`default config`), or interrupts the restart and stops.

Table 20: Buttons (section 1 of 3)

Button	Meaning
Export...	Opens the "Export..." dialog. There you save the device configuration of the selected table entry as an XML file on the PC or on a server in the network: The device gives you the following options for saving the device configuration: ▶ Download to PC To save the XML file on a PC, click " … " and select the directory there. ▶ SFTP or SCP download The device allows you to transfer the device configuration from the device to your PC using SFTP or SCP. □ On your PC, open an SFTP or SCP client, e.g. WinSCP. □ Use the SFTP or SCP client to open a connection to the device. □ Switch to directory `/nv/cfg` on the device. □ Transfer the file with the ending *.xml to your PC.
Import...	Opens the "Import..." dialog. There you select a device configuration saved as an XML file in order to import it to the device. □ In the "Storage Type" field you specify the storage location for the device configuration to be imported. □ In the "Name" field you specify the name for the device configuration to be imported. The device provides you with the following options for importing the device configuration: ▶ File upload If the device configuration to be imported is on your PC or on a network drive, click " … " and select the file with the ending `*.xml` there. ▶ SFTP or SCP upload The device allows you to transfer the device configuration from your PC to the device using SFTP or SCP: □ On your PC, open an SFTP or SCP client, e.g. WinSCP. □ Use the SFTP or SCP client to open a connection to the device. □ Transfer the device configuration with the ending `*.xml` to the directory `/nv/cfg` on the device. The device only accepts an encrypted device configuration if the password used there matches the password set in the "Configuration Encryption" frame.
View...	Displays the device configuration of the selected table entry in a dialog window. This text display gives you an overview of the configuration parameters.
Save As...	Opens the "Save As..." dialog. Transfers the saved device configuration from the volatile memory (`RAM`) to the non-volatile memory (`NVM`). You can specify the name of the device configuration by selecting a table entry and clicking "Save As...".

Table 20: Buttons (section 2 of 3)

Button	Meaning
Back to factory defaults...	Resets the settings of the device to the state on delivery: ▶ The device deletes all the saved settings from the volatile memory (`RAM`) and from the non-volatile memory (`NVM`). ▶ If an external memory is connected, the device also deletes all the saved settings from the external memory (`ENVM`). ▶ Then the device restarts.
Help	Opens the online help.

Table 20: Buttons (section 3 of 3)

1.5 External Memory

With this dialog you can check the operating condition of the external memory (`ENVM`) and define settings for saving the device configuration and for automatic software updates.

■ Table

Parameters	Meaning
Type	Shows the type of the connected external memory. Possible values: ▶ `SD` SD memory card (ACA31) ▶ `USB` USB stick (ACA21)
Status	Shows the operating state of the connected external memory. Possible values: ▶ `notPresent` No external memory connected. ▶ `removed` Someone has removed the external memory from the device during operation. ▶ `ok` The external memory is connected and ready for operation. ▶ `outOfMemory` The memory space is occupied on the external memory. ▶ `genericErr` The device has detected an error.

Table 21: "External Memory" dialog, table (section 1 of 3)

Parameters	Meaning
Enable Automatic Software Update	Activates/deactivates the option to automatically load an updated device software from the external memory during the device start and copy it to the device. Possible values: ▶ `Selected` (default setting) Automatic updates of the device software from the external memory are possible. To update the device software automatically, proceed as follows: □ Copy the software image of the device software to the external memory. □ Copy a text file "startup.txt" with the content `autoUpdate=FILENAME` , e.g. HiSecOS-EAGLE-01000.bin, to the external memory. You will find more information in the “Basic Configuration” user manual. ▶ `Not selected` Automatic software updates from the external memory are deactivated.
Config Priority	Defines whether the device loads the device configuration from the external memory (`ENVM`) or from the non-volatile memory (`NVM`) during a restart. Possible values: ▶ `disable` The device loads the device configuration from the non-volatile memory (`NVM`). ▶ `first`, `second`, `third` The device loads the device configuration from the external memory (`ENVM`). – If multiple external memories are connected, the device loads the device configuration from the memory that is designated with the value `first`. If the device does not find any device configuration there, it loads the device configuration from the next external memory. – If the device does not find the device configuration on any of the connected external memories, it loads the device configuration from the non-volatile memory (`NVM`). **Note:** The device configuration from the external memory (ENVM) overwrites the device configuration in the non-volatile memory (NVM) of the device.

Table 21: "External Memory" dialog, table (section 2 of 3)

Parameters	Meaning
Auto-save config on envm	Activates/deactivates the automatic saving of a backup of the device configuration on the external memory. Possible values: ▶ `Selected` (default setting) The device creates a backup of the device configuration on the external memory when you click "Save" in the `Basic Settings:Load/Save` dialog. ▶ `Not selected` The device does not create a backup of the device configuration.

Table 21: "External Memory" dialog, table (section 3 of 3)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 22: Buttons

1.6 Port Configuration

This dialog allows you to configure the device ports individually. This dialog shows for each device port the current operating mode, link status, bit rate and duplex mode.

■ Table

Parameters	Meaning
Port	Device port to which the table entry relates.
Name	Name of the device port. Enter the name of your choice. Possible values: ▶ 0..64 alphanumeric characters
Port on	Activates/deactivates the device port. Possible values: ▶ `Selected` (default setting) The device port is activated. ▶ `Not selected` The device port is deactivated. The device port does not send or receive any data.
Power State (Port off)	Defines whether the device port is physically switched on or off after the "Port on" function is deactivated. Possible values: ▶ `Not selected` (default setting) The device port is physically switched off. ▶ `Selected` The device port remains physically switched on. A connected device receives an active link.
Auto Power Down	Defines how the device port behaves when no cable is connected. Possible values: ▶ `no-power-save` (default setting) The device port remains activated. ▶ `auto-power-down` The device port switches to the energy-saving mode. ▶ `unsupported` The device port does not support this function and remains activated.

Table 23: "Port Configuration" dialog, table (section 1 of 3)

Parameters	Meaning
Automatic Configuration	Activates/deactivates the automatic configuration of the device port. Possible values: ▶ `Selected` (default setting) This setting has priority over the manual configuration of the device port. The device port negotiates the operating mode independently using autonegotiation and detects the devices connected to the TP port automatically (Auto Cable Crossing). After the function is switched on, it takes a few seconds for the device port to set the operating mode. ▶ `Not selected` The device port works with the values you defined in the "Manual Configuration" column and the "Manual Cable Crossing (Auto. Conf. off)" column.
Manual Configuration	Defines the operating mode of the device port. Prerequisite: The automatic configuration of the device port is deactivated. The operating modes available depend on the media module. Possible values: ▶ `10 Mbit/s HDX` Half duplex connection ▶ `10 Mbit/s FDX` Full duplex connection ▶ `100 Mbit/s HDX` Half duplex connection ▶ `100 Mbit/s FDX` (default setting on TP ports) Full duplex connection ▶ `1000 Mbit/s FDX` (default setting on optical ports or TP-SFP ports) Full duplex connection
Link/Current Settings	Displays the current operating mode of the device port. Possible values: ▶ `-` No cable connected, no link. ▶ `10 Mbit/s HDX` Half duplex connection ▶ `10 Mbit/s FDX` Full duplex connection ▶ `100 Mbit/s HDX` Half duplex connection ▶ `100 Mbit/s FDX` Full duplex connection ▶ `1000 Mbit/s FDX` Full duplex connection

Table 23: "Port Configuration" dialog, table (section 2 of 3)

Parameters	Meaning
Manual Cable Crossing (Auto. Conf. off)	Defines the devices connected to a TP port. Prerequisite: The automatic configuration of the device port is deactivated. Possible values: ▶ `mdi` The device switches the send and receive line pairs at the device port. ▶ `mdix` (default setting on TP ports) The device does not switch any line pairs at the device port. ▶ `auto-mdix` The device detects the send and receive line pairs of the connected device and automatically adapts to them. Example: When you connect a terminal device with a crossed cable, the device automatically resets the port from MDIX to MDI. ▶ `unsupported` (default setting on optical ports or TP-SFP ports) The device port does not support this function.
Flow Control	Activates/deactivates the flow control on the device port. Possible values: ▶ `Not selected` Flow control on the device port is deactivated. ▶ `Selected` (default setting) The sending and evaluating of pause data packets (full-duplex operation) or collisions (half-duplex operation) is activated on the port. □ To switch on the flow control in the device, also switch on the "Activate Flow Control" function in the `Switching:Global` dialog. □ Additionally activate the flow control on the port of the device connected with this port. On an uplink port, activating the flow control can possibly cause undesired sending breaks in the higher-level network segment (“wandering backpressure”). When you are using a redundancy function, you deactivate the flow control on the participating device ports. If the flow control and the redundancy function are active at the same time, there is a risk that the redundancy function will not operate as intended.

Table 23: "Port Configuration" dialog, table (section 3 of 3)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 24: Buttons

1.7 Restart

This dialog allows you to restart the device, reset port counters and address tables, and delete log files.

Restart

Button	Meaning
Cold start...	Opens the "Restart" dialog to initiate a cold start of the device. When the dialog is confirmed, the device reloads the software from the non-volatile memory, restarts, and performs a self-test before loading the operating system.

Table 25: "Restart" dialog, "Restart" frame

Note: During the restart, the device does not transfer any data, and it cannot be accessed via the Web-based interface or other management systems.

Buttons

Button	Meaning
Reset MAC Address Table	Removes the MAC addresses from the forwarding table that the device set up based on the received data packets. In the `Switching:Filter for MAC Addresses` dialog, these MAC addresses are designated with the setup status `learned`.
Reset ARP Table	In the `Diagnostics:ARP` dialog, removes the dynamically setup addresses from the table.
Reset port counters	In the `Diagnostics:Ports:Port Statistics` dialog, resets all values to `0`.
Delete Log File	Removes the logged events from the log file, see the `Diagnostics:Report:System Log` dialog.
Delete Persistent Log File	Removes the log files held on the external memory, see the `Diagnostics:Report:Persistent Event Log` dialog.
Delete firewall table	Removes the information about open connections from the state table of the firewall. In the process, the device may possibly interrupt open connections.
Help	Opens the online help.

Table 26: Buttons

2 Security

With this menu you can configure safety-related settings.

The menu contains the following dialogs:

- User Management
- Authentication List
- Management Access
- RADIUS
- Pre-login Banner

2.1 User Management

The device allows authorized users to access its management functions via CLI, the graphical user interface and SNPMv3.

This dialog allows you to set up and manage user accounts locally on the device. The dialog also includes the following settings:

- Settings for the login.
- Settings for saving the passwords.
- Define policy for valid passwords.

Every user account is linked to an authorization profile that regulates the access to the individual functions of the device. Depending on the planned activity for the respective user, you assign a predefined authorization profile to the user. The device differentiates between the following authorization profiles.

Authorization	Description	Authorized for the following activities
Administrator	The user is authorized to monitor and administer the device.	All activities with read/write access, including the following activities reserved for an administrator: ▶ Add, modify or delete user accounts ▶ Activate, deactivate or unlock user accounts ▶ Change all passwords ▶ Configure password management ▶ Set or change system time ▶ Load files to the device, e.g. device configurations, certificates or software images ▶ Reset settings and security-related settings to the state on delivery ▶ Configure RADIUS server and authentication lists ▶ Apply CLI scripts ▶ Switch CLI logging and SNMP logging on and off ▶ External memory activation and deactivation ▶ System monitor activation and deactivation ▶ Switch the services for the management access (e. g. SNMP) on and off. ▶ Configure access restrictions to the user interfaces or the CLI based on the IP addresses
Guest	The user is authorized to monitor the device - with the exception of security-related settings.	Monitoring activtities with read access.
Operator	The user is authorized to monitor and configure the device - with the exception of security-related settings.	All activities with read/write access, with the exception of the above-named activities, which are reserved for an administrator:
Unauthorized	No access to the device possible. ▶ As an administrator you assign this authorization to temporarily lock a user account. ▶ The device assigns this authorization to a user account if an error occurs when assigning a different authorization profile.	No activities allowed.

Table 27: Authorization profiles for user accounts

Configuration

This frame allows you to define settings for the login.

Parameters	Meaning
Number of Login Attempts	Number of login attempts possible. Possible values: ▶ `0..5` (default setting: `0`) If the user makes one more unsuccessful login attempt, the device locks access for the user. The device only allows users with the `Administrator` authorization to remove the lock. The value `0` deactivates the lock. The user can make unlimited attempts to login.

Table 28: "User Management" dialog, "Configuration" frame

■ Password policy

This frame allows you to define the policy for valid passwords. The device checks every new password and password change according to this policy.
The settings affect the "Password" field. The prerequisite is that the "Policy Check" must be checkmarked.

Parameters	Meaning
Minimum Password Length	The device accepts the password if it contains at least the number of characters specified here. The device checks the password according to this setting, regardless of the setting for the "Policy Check" checkbox. Possible values: ▶ `6..64` (default setting: `6`)
Minimum Upper Cases	The device accepts the password if it contains at least as many upper-case letters as specified here. Possible values: ▶ `0..16` (default setting: `1`) The value `0` deactivates this setting.
Minimum Lower Cases	The device accepts the password if it contains at least as many lower-case letters as specified here. Possible values: ▶ `0..16` (Default setting: `1`) The value `0` deactivates this setting.
Minimum Numbers	The device accepts the password if it contains at least as many numbers as specified here. Possible values: ▶ `0..16` (default setting: `1`) The value `0` deactivates this setting.
Minimum Special Characters	The device accepts the password if it contains at least as many special characters as specified here. Possible values: ▶ `0..16` (default setting: `1`) The value `0` deactivates this setting.

Table 29: "User Management" dialog, "Password Policy" frame

Table

Every user requires an active user account to gain access to the management functions of the device. The table allows you to set up and manage user accounts.

To change settings click the desired parameter in the table and modify the value.

Parameters	Meaning
User Name	Unique name for the user account.
Active	Activates/deactivates the user account. Possible values: ▶ `selected` The user account is activated. The user has access to the management functions. ▶ `not selected` The user account is deactivated. The user has no access to the management functions. If only one user account with the `administrator` authorization exists in the user accounts that are set up, this user account is always activated.
Password	Password with which the user authenticates themselves. Possible values: ▶ 6..64 alphanumeric characters You define the minimum length of the password in the "Password Policy" frame. ▶ including the following special characters: !#$%&'()*+,-./:;<=>?@[\\]^_`{}~ The device differentiates between upper and lower case. Depending on the setting in the "Policy Check" checkbox, the device checks the password based on the policy. The device checks the minimum length of the password regardless of the setting in the "Policy Check" checkbox.

Table 30: "User Management" dialog, table (section 1 of 3)

Parameters	Meaning
Authorization	Defines the role of the user for access to the management functions of the device. Possible values: ▶ `guest` The user is authorized to monitor the device. ▶ `operator` The user is authorized to monitor and configure the device - with the exception of security-related settings. ▶ `administrator` The user is authorized to monitor and configure the device. ▶ `unauthorized` – As an administrator you assign this authorization to temporarily lock a user account. – The device assigns this authorization to a user account if an error occurs when assigning a different authorization profile.
User locked	Defines the authorization of the user for access to the management functions of the device. Possible values: ▶ `Selected` The user has no access to the management functions. – The user has made too many attempts to login. – The device only allows users with the `Administrator` authorization to remove the lock. ▶ `Not selected` The user has access to the management functions.
Policy Check	Defines whether the device checks every new password and password change according to the policy. Possible values: ▶ `Selected` The device checks every new password and password change according to this policy. ▶ `Not selected` The device accepts the password regardless of the policy.
SNMP Auth Type	Authentication protocol with which the user account authenticates itself for access via SNMPv3. Possible values: ▶ `hmacmd5` The user account authenticates itself with protocol HMAC-MD5. ▶ `hmacsha` The user account authenticates itself with protocol HMAC-SHA.

Table 30: "User Management" dialog, table (section 2 of 3)

Parameters	Meaning
SNMP Encryption Type	Encryption protocol which the user account uses for access via SNMPv3. Possible values: ▶ `none` No encryption ▶ `des` DES encryption ▶ `aesCfb128` AES-128 encryption

Table 30: "User Management" dialog, table (section 3 of 3)

■ New Entry

This dialog allows you to set up a new user account.
To open the dialog, click the "Create" button.

Parameters	Meaning
User Name	Unique name for the user account. Possible values: ▶ 1..32 alphanumeric characters
Enabled	Activates/deactivates the user account. Possible values: ▶ `Not selected` (default setting) The user account is deactivated. The user has no access to the management functions. ▶ `Selected` The user account is activated. The user has access to the management functions.
Password	Password with which the user authenticates themselves. Possible values: ▶ 6..64 alphanumeric characters You define the minimum length of the password in the "Password Policy" frame. ▶ including the following special characters: !#$%&'()*+,-./:;<=>?@[\\]^_`{}~ The device differentiates between upper and lower case. Depending on the setting in the "Display Password" checkbox, the device displays the password in clear text. Depending on the setting in the "Policy Check" checkbox, the device checks the password based on the policy. The device checks the minimum length of the password regardless of the setting in the "Policy Check" checkbox.
Display Password	Define how the device displays the password. Possible values: ▶ `Not selected` (default setting) The "Password" field displays *** (asterisks) instead of the password. ▶ `Selected` The "Password" field displays the password in clear text.

Table 31: "New Entry" dialog (section 1 of 3)

Parameters	Meaning
Authorization	Defines the role of the user for access to the management functions of the device. Possible values: ▶ guest The user is authorized to monitor the device. ▶ operator The user is authorized to monitor and configure the device - with the exception of security-related settings. ▶ administrator The user is authorized to monitor and configure the device. ▶ unauthorized – As an administrator you assign this authorization to temporarily lock a user account. – The device assigns this authorization to a user account if an error occurs when assigning a different authorization profile.
User locked	Defines the authorization of the user for access to the management functions of the device. Possible values: ▶ Selected The user has no access to the management functions. – The user has made too many attempts to login. – The device only allows users with the Administrator authorization to remove the lock. ▶ Not selected (default setting) The user has access to the management functions.
Policy Check	Defines whether the device checks every new password and password change according to the policy. Possible values: ▶ Not selected (default setting) The device accepts the password regardless of the policy. ▶ Selected The device checks every new password and password change according to this policy.
SNMP Auth Type	Authentication protocol with which the user account authenticates itself for access via SNMPv3. Possible values: ▶ hmacmd5 (default setting) The user account authenticates itself with protocol HMAC-MD5. ▶ hmacsha The user account authenticates itself with protocol HMAC-SHA.

Table 31: "New Entry" dialog (section 2 of 3)

Parameters	Meaning
SNMP Encryption Type	Encryption protocol which the user account uses for access via SNMPv3. Possible values: ▶ `none` No encryption ▶ `des` (default setting) DES encryption ▶ `aesCfb128` AES-128 encryption

Table 31: "New Entry" dialog (section 3 of 3)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Set and back	Transfers the changes to the volatile memory (`RAM`) of the device and goes back to the previous dialog.
Back	Displays the previous dialog again. Changes are lost.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Remove	Removes the selected table entry.
Create	Adds a new table entry.
Help	Opens the online help.

Table 32: Buttons

■ Factory setting user accounts

In the state on delivery, the user accounts `admin` and `user` are set up on the device.

Parameters	Value in the state on delivery	
User Name	`admin`	`user`
Password	`private`	`public`
User locked	`off`	`off`
Password Change Permission	`on`	`off`
Policy Check	`off`	`off`
SNMP Auth Type	`hmacmd5`	`hmacmd5`
SNMP Encryption Type	`des`	`des`

Table 33: Default settings for the factory setting user accounts

Note: Change the password for the `admin` user account before making the device available in the network.

2.2 Authentication List

The device only allows authorized users to access its management functions. The device authenticates and authorizes the users remotely with the RADIUS server or locally with the user accounts that have been set up.

You use authentication lists to define a policy that the device uses to authenticate and authorize users.

This dialog allows you to manage the authentication lists. Users can access the management functions of the device via different applications (consoles, Web interfaces, etc.). You can create a separate authentication list for each application.

Table

Parameters	Meaning
Name	Unique name for the authentication list
Policy 1 Policy 2 Policy 3 Policy 4 Policy 5	Authentication method with which the device authenticates a user who logs in. If the authentication fails, the device uses the method in the next policy. Sequence: Policy 1, policy 2, etc. Possible values: ▶ `local` The device uses the user management to authenticate the user. See the `Security:User Management` dialog. ▶ `radius` The device uses a RADIUS server to authenticate the user. See the `Security:RADIUS` dialog. ▶ `reject` The device rejects the authentication request from the user.
Dedicated Applications	Shows the applications that are allocated to the authentication list. Every application can be allocated to exactly one authentication list at the same time.
Active	Activates/deactivates the user account. Possible values: ▶ `selected` The authentication list is activated. The device uses this authentication list to authenticate users. ▶ `not selected` The authentication list is deactivated. The device ignores this authentication list.

Table 34: "Authentication List" dialog, table

To change an authentication list, click the desired parameter in the table and modify the value. To allocate an application to the authentication list or remove the allocation, select the desired row and click the "Allocate Applications" button.

Note: If the table does not contain an authentication list, it is then only possible to access the management functions using CLI via the V.24 interface of the device. The prerequisite here is a locally set up user account.

■ New Entry

This dialog allows you to set up a new authentication list.
To open the dialog, click the "Create" button.

Parameters	Meaning
Name	Unique name for the authentication list Possible values: ▶ 1..32 alphanumeric characters
Policy 1 Policy 2 Policy 3 Policy 4 Policy 5	Authentication method with which the device authenticates a user who logs in. If the authentication fails, the device uses the method in the next policy. Sequence: Policy 1, policy 2, etc. Possible values: ▶ `local` The device uses the user management to authenticate the user. See the `Security:User Management` dialog. ▶ `radius` The device uses a RADIUS server to authenticate the user. See the `Security:RADIUS` dialog. ▶ `reject` The device rejects the authentication request from the user.
Active	Activates/deactivates the user account. Possible values: ▶ `on` The authentication list is activated. The device uses this authentication list to authenticate users. ▶ `off` (default setting) The authentication list is deactivated. The device ignores this authentication list.

Table 35: "New Entry" dialog

■ Allocate Applications

This dialog allows you to allocate one or more applications (consoles, Web interface, etc.) to the selected authentication list, or to remove the allocation.
To open the dialog, click the "Allocate Applications" button.
You use the buttons to allocate available applications or remove the allocation.

Parameters	Description
Possible Applications	This column contains the applications with which users can access the management functions of the device. The applications may possibly be allocated to other authentication lists. Every application can be allocated to exactly one authentication list at the same time. If you allocate an application that is already allocated to another authentication list, you thus remove the original allocation. Possible values: ▶ `Console (V.24)` ▶ `SSH` ▶ `WebInterface`
Dedicated Applications	This column contains the applications that are allocated to the authentication list.

Table 36: "Allocate Applications" dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Set and back	Transfers the changes to the volatile memory (RAM) of the device and goes back to the previous dialog.
Back	Displays the previous dialog again. Changes are lost.
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Remove	Removes the selected table entry.
Create	Adds a new table entry.
Allocate Applications	Displays the "Allocate Applications" dialog.
Help	Opens the online help.
>	Moves the selected entry to the right column.
>>	Moves all entries to the right column.
<	Moves the selected entry to the left column.
<<	Moves all entries to the left column.

Table 37: Buttons

2.3 Management Access

This dialog allows you to set up the server services with which users or applications can access the management functions of the device. You also have the option of restricting the access for IP address ranges and individual management services.

The menu contains the following dialogs:
- Server
- SNMPv1/v2 Community
- IP Access Restriction
- Web
- CLI

2.3.1 Server

This dialog allows you to set up the server services with which users or applications can access the management functions of the device.

The dialog contains the following tabs:
- Server: SNMP
- Server: HTTPS
- Server: SSH

2.3.2 Server: SNMP

This tab allows you to define settings for the SNMP server of the device and to switch on/off the access to the device with different SNMP versions.

The SNMP server enables access to the management functions of the device with SNMP-based applications, e.g. with the graphical user interface.

■ Configuration

Parameters	Meaning
SNMPv1 enabled	Activates/deactivates the access to the device with SNMP version 1. Possible values: ▶ `Selected` Access activated. ▶ `Not selected` (default setting) Access deactivated. You define the community name in the `Security:Management Access:SNMPv1/v2 Community` dialog.
SNMPv2 enabled	Activates/deactivates the access to the device with SNMP version 2. Possible values: ▶ `Selected` Access activated. ▶ `Not selected` (default setting) Access deactivated. You define the community name in the `Security:Management Access:SNMPv1/v2 Community` dialog.
SNMPv3 enabled	Activates/deactivates the access to the device with SNMP version 3. Possible values: ▶ `Selected` (default setting) Access activated. ▶ `Not selected` Access deactivated. This function is used, for example, by the Industrial HiVision network management software to make changes to the settings.

Table 38: "Server" dialog, "SNMP" tab, "Configuration" frame

Parameters	Meaning
Port number	Defines the number of the UDP port from which the SNMP server receives requests from clients. Possible values: ▶ `1..65535` (default setting: `161`) Exception: Port `2222` is reserved for internal functions. To get the server to use the new port after a change, you proceed as follows: □ Click on "Set". □ Select the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save". □ Restart the device.

Table 38: "Server" dialog, "SNMP" tab, "Configuration" frame (Cont.)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 39: Buttons

2.3.3 Server: HTTPS

This tab allows you to define settings for the HTTPS server of the device and to switch the server on/off.

The HTTP server provides the graphical user interface (GUI) via an encrypted HTTP connection. The graphical user interface communicates with the device based on SNMP via the encrypted HTTP connection and enables access to the management functions.

The device supports up to 10 simultaneous connections via HTTPS.

A digital certificate is required for the encryption of the HTTP connection. The device allows you to create this certificate yourself or to load an existing certificate onto the device.

■ Operation

Parameters	Meaning
Operation	When the function is switched on, the device supplies the graphical user interface (GUI) via an encrypted HTTP connection. Possible values: ▶ `Off` Server is deactivated. The management functions of the device can only be accessed via the Command Line Interface (CLI). ▶ `On` (default setting) Server is activated. You can access the management functions of the device via HTTPS. The device can then only be started if there is a certificate on the device.

Table 40: "Server" dialog, "HTTPS" tab, "Operation" frame

Note: When you switch off the server, the connection between the graphical user interface (GUI) and the device is interrupted. To continue working with the graphical user interface, switch the server on again via the Command Line Interface (CLI).

■ Configuration

Parameters	Meaning
Listen TCP Port	Defines the number of the TCP port on which the server receives requests from clients. Possible values: ▶ `1..65535` (default setting: `443`) Exception: Port `2222` is reserved for internal functions. To apply the changes, reset the server by turning it off and then on. In the process, the device terminates open connections to the server.

Table 41: "Server" dialog, "HTTPS" tab, "Configuration" frame

■ Certificate

Parameters	Meaning
Present	Shows whether the digital certificate is present in the device. Possible values: ▶ `Selected` The certificate is present. ▶ `Not selected` The certificate has been removed.
Create	Creates a digital certificate on the device. To get the server to use this certificate, you click "Set" and restart the server. You can only restart the server via the Command Line Interface (CLI). Alternatively, you can copy your own certificate to the device - see the "Certificate Import" dialog.
Delete	Deletes the digital certificate. To permanently remove the certificate from the device, save the changes. In the process, the device switches off the HTTPS server.

Table 42: "Server" dialog, "HTTPS" tab, "Certificate" frame

Note: In the Web browser, a warning appears when you are loading the graphical user interface if you are using a certificate that has not been verified by a certifying organization. To load the graphical user interface, add an exception rule for the certificate in the Web browser.

■ Certificate Import

Parameters	Meaning
URL	Defines the path and file name of the certificate. X.509 certificates (PEM) are permitted. The device gives you the following options for copying the certificate to the device: ▶ File upload If the certificate is on your PC or on a network drive, click " … " and select the file that contains the signature key. ▶ SFTP or SCP upload The device allows you to transfer the certificate from your PC to the device using SFTP or SCP: □ On your PC, open an SFTP or SCP client, e.g. WinSCP. □ Use the SFTP or SCP client to open a connection to the device. □ Transfer the certificate file to directory `/upload/https-cert` on the device. When the file is completely transferred, the device starts installing the certificate. If the installation was successful, the device creates an `ok` file in directory `/upload/https-cert` and deletes the certificate file. □ To get the server to use this certificate, you restart the server. You can only restart the server via the Command Line Interface (CLI).
…	Shows the "Open" dialog. Here you select the certificate file to be copied if the file is located on your PC or on a network drive.
Import	Copies the certificate defined in the "File" field to the device. To get the server to use this certificate, you click "Set" and restart the server. You can only restart the server via the Command Line Interface (CLI).

Table 43: "Server" dialog, "HTTPS" tab, "Certificate Import" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 44: Buttons

2.3.4 Server: SSH

This tab allows you to switch the SSH server on/off in the device and define its settings.

The server works with SSH version 2. The SSH server enables access to the management functions of the device with the Command Line Interface via an encrypted connection (secure shell).
To access the device and the connected external memory using SFTP or SCP, you also need access to the SSH server. With an SFTP or SCP client, e.g. WinSCP, you have the option to load configuration files or a software update to the device.

The SSH server identifies itself to the clients using its public RSA or DSA key. When first setting up the connection, the client program shows the user the fingerprint of this key. The fingerprint contains a hexadecimal number sequence that is easy to check. When you make this number sequence available to the users via a reliable channel, they have the option to compare both fingerprints. If the number sequences match, the client is connected to the correct server.

The device allows you to create the private and public keys (host keys) required for RSA and DSA directly on the device. Otherwise you have the option to copy your own keys to the device in PEM format.

■ Operation

Parameters	Meaning
Operation	If the function is switched on, encrypted access to the management functions of the device is possible via the Command Line Interface (CLI). Possible values: ▶ `Off` Server is deactivated. ▶ `On` (default setting) Server is activated. You can access the management functions of the device via SSH. The server can only be started if there is an RSA or DSA signature on the device. When the function is switched off, existing connections remain in place. However, the device prevents new connections from being set up.

Table 45: "Server" dialog, "SSH" tab, "Operation" frame

■ Configuration

Parameters	Meaning
Listen TCP Port	Defines the number of the TCP port on which the server receives requests from clients. Possible values: ▶ `1..65535` (default setting: `22`) Exception: Port `2222` is reserved for internal functions. The server restarts automatically after the port is changed. Existing connections remain in place.
Session Count	Shows how many connections to the server are currently set up.
Max. Number of Sessions	Defines the maximum number of connections to the server that can be set up simultaneously. Possible values: ▶ `1..3` (default setting: `3`)
Session Timeout [min]	Defines the timeout in minutes. After the device has been inactive for this time it ends the session for the user logged on. Possible values: ▶ `1..160` (default setting: `5`) The value `0` deactivates the function. The user remains logged on when inactive.

Table 46: "Server" dialog, "SSH" tab, "Configuration" frame

■ Fingerprint

The fingerprint is an easily verified hexadecimal number sequence that uniquely identifies the RSA or DSA key (host key) of the SSH server.

Parameters	Meaning
DSA	Number sequence of the public DSA key of the server.
RSA	Number sequence of the public RSA key of the server.

Table 47: "Server" dialog, "SSH" tab, "Fingerprint" frame

After importing a new RSA or DSA key, the device continues to display the existing fingerprint until you restart the server.

■ Signature

Parameters	Meaning
DSA Present	Shows whether a DSA key (host key) is present in the device. Possible values: ▶ `selected` A key is present. ▶ `not selected` No key is present.
RSA Present	Shows whether an RSA key (host key) is present in the device. Possible values: ▶ `selected` A key is present. ▶ `not selected` No key is present.
Create	Creates a key (host key) on the device. The device only creates the key when the server is deactivated. Length of the key created: ▶ 2048 bit (RSA) ▶ 1024 bit (DSA) To get the server to use the key created, you click "Set". Then you switch the server `on`. Alternatively, you can copy your own key to the device in PEM format - see the "Import" frame.
Delete	Removes the key (host key) from the device. To permanently remove the key from the device, click "Set". Until you restart the server, the existing connections remain in place. However, the device prevents new connections from being set up.

Table 48: "Server" dialog, "SSH" tab, "Signature" frame

■ Key Import

Parameters	Meaning
URL	Defines the path and file name of your own DSA/RSA key (host key). The device accepts the DSA/RSA key if it has the following key length: ▶ 2048 bit (RSA) ▶ 1024 bit (DSA) The device gives you the following options for copying the key to the device: ▶ File upload If the key is on your PC or on a network drive, click " … " and select the file that contains the key (host key). ▶ SFTP or SCP upload The device allows you to transfer the key from your PC to the device using SFTP or SCP: □ On your PC, open an SFTP or SCP client, e.g. WinSCP. □ Use the SFTP or SCP client to open a connection to the device. □ Transfer the file that contains the key to the directory `/upload/ssh-key` on the device. When the file is completely transferred, the device starts installing the key. If the installation was successful, the device creates an `ok` file in directory `/upload/ssh-key` and deletes the file that contains the key. □ To get the server to use this key, you restart the server.
…	Shows the "Open" dialog. Here you select the key to be copied if the file is located on your PC or on a network drive.
Import	Copies the key (host key) defined in the "File" field to the device. To get the server to use this key, you click "Set" and restart the server.

Table 49: "Server" dialog, "SSH" tab, "Key Import" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 50: Buttons

2.3.5 SNMPv1/v2 Community

With this dialog you can define the community name for SNMPv1/v2 applications.

Applications send requests via SNMPv1/v2 with a community name in the SNMP packet header. Depending on the community name, the application gets read authorization or read and write authorization for the device.

You activate the access to the device via SNMPv1/v2 in the Security:Management Access:Server dialog.

■ Table

Parameters	Meaning
Community	Shows the authorization for SNMPv1/v2 applications to the device: ▶ Write For requests with the community name entered beside this, the application gets read and write authorization for the device. ▶ Read For requests with the community name entered here, the application gets read authorization for the device.
Name	Defines the community name for the authorization entered beside it. Possible values: ▶ 0..32 alphanumeric characters ▶ including spaces and the following special characters: !#$%&'()*+,-./:;<=>?@[\\]^_`{}~ ▶ private (default setting for read and write authorization) ▶ public (default setting for read authorization)

Table 51: "SNMPv1/v2 Community" dialog, table

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 52: Buttons

2.3.6 IP Access Restriction

This dialog enables you to restrict the access to the management functions of the device to specific IP address ranges and selected IP-based applications.

- If the function is switched off, you can access the management functions of the device from any IP address and via all applications.
- If the function is switched on, the access is restricted. You can only access the management functions under the following conditions:
  - At least one table entry is activated.
    and
  - You are accessing the device with a permitted application from a permitted IP address range.

■ Operation

Parameters	Meaning
Operation	If the function is switched on, the access to the management functions of the device is restricted. Possible values: ▶ `Off` (default setting). ▶ `On` Access to the management functions of the device is restricted.

Table 53: "IP Access Restriction" dialog, "Operation" frame

Note: Before switching on the function, make sure that at least one active entry in the table allows you access: Otherwise the connection to the device terminates when you change the device configuration. It is then only possible to access the management functions using CLI via the V.24 interface of the device.

■ Table

You have the option of defining up to 16 table entries and activating them separately.

Parameters	Meaning
Index	Shows a sequential number to which the table entry relates. The device automatically defines this number. Possible values: ▶ `1..16` When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap.
IP Address Range	Specifies the IP address range for which you define the access to the management functions with this table entry. Possible values: ▶ Valid IPv4 address and netmask in CIDR notation ▶ `0.0.0.0/0` (default setting for all newly created entries)
HTTPS	Activates/deactivates the HTTPS access. Possible values: ▶ `Selected` (default setting) Access is activated for the adjacent IP address range. ▶ `Not selected` Access is deactivated.
SNMP	Activates/deactivates the SNMP access. Possible values: ▶ `Selected` (default setting) Access is activated for the adjacent IP address range. ▶ `Not selected` Access is deactivated.
SSH	Activates/deactivates the SSH access. Possible values: ▶ `Selected` (default setting) Access is activated for the adjacent IP address range. ▶ `Not selected` Access is deactivated.
Active	Activates/deactivates the table entry. Possible values: ▶ `Selected` (default setting) Table entry is activated. The device restricts access to its management functions to the adjacent IP address range and the selected IP-based applications. ▶ `Not selected` Table entry is deactivated.

Table 54: "IP Access Restriction" dialog, table

In the state on delivery, there is a default entry in the table for the IP address range `0.0.0.0/0`, in which the access for all applications is activated. This table entry allows you access to the device regardless of your location, e.g. to initially configure the function. You have the option to change or delete this table entry. When you create a new table entry it has the same properties.

Note: To start the graphical user interface in a Web browser, you require the "HTTPS" service.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 55: Buttons

2.3.7 Web

With this dialog you can define settings for the graphical user interface (Web-based interface).

■ Configuration

Parameters	Meaning
Web Interface Session Timeout [min]	Defines the timeout in minutes. After the device has been inactive for this time it ends the session for the user logged on. Possible values: ▶ `0..160` (default setting: `5`) The value `0` deactivates the function, and the user remains logged on when inactive.

Table 56: "Web" dialog, "Configuration" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 57: Buttons

2.3.8 CLI

With this dialog you can define settings for the Command Line Interface (CLI). You will find detailed information on the Command Line Interface in the “Command Line Interface” reference manual.

The dialog contains the following tabs:

- CLI: Global
- CLI Login banner

2.3.9 CLI: Global

This tab allows you to change the CLI prompt and to define the automatic closing of sessions via the V.24 interface when they have been inactive.

■ Configuration

Parameters	Meaning
Login Prompt	Defines the character string that the device displays in the Command Line Interface (CLI) at the start of every command line. Possible values: ▶ 0..32 alphanumeric characters ▶ including spaces and the following special characters: !#$%&'()*+,-./:;<=>?@[\\]^_`{}~ ▶ (EAGLE) (default setting) Changes to this setting are immediately effective in the active CLI session.
V.24 Timeout [min]	Defines the time in minutes after which the device automatically closes the session of a logged on user in the Command Line Interface via the V.24 interface when it has been inactive. Possible values: ▶ 0..160 (default setting: 5) The value 0 deactivates the function, and the user remains logged on when inactive. For Telnet and SSH, you define the timeout in the Security:Management Access:Server dialog.

Table 58: "CLI" dialog, "Global" tab, "Configuration" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 59: Buttons

2.3.10 CLI Login banner

This tab page allows you to replace the CLI start screen with your own text.

In the state on delivery, the CLI start screen shows information about the device, such as the software version and the device settings. With the function on this tab page, you deactivate this information and replace it with an individually defined text.

To display your own text in the CLI and in the graphical user interface before the login, you use the `Security:Pre-login Banner` dialog.

■ Operation

Parameters	Meaning
Operation	When this function is switched on, the device shows the text information defined in the "Banner Text" field to all the users that login to the device via the Command Line Interface (CLI). When the function is switched off, the CLI start screen shows information about the device. The text information in the "Banner Text" field is kept. Possible values: ▶ `Off` (default setting). ▶ `On`

Table 60: "CLI" dialog, "Login Banner" tab, "Operation" frame

■ Banner Text

Parameters	Meaning
Banner Text	Defines the character string that the device displays in the Command Line Interface at the start of every command line. Possible values: ▶ 0..1024 alphanumeric characters ▶ including spaces, tabs, line breaks and the following special characters: !#$%&'()*+,-./:;<=>?@[\\]^_`{}~
Remaining Characters	Shows how many characters are still remaining in the "Banner Text" field for the text information.

Table 61: "CLI" dialog, "Login Banner" tab, "Banner Text" frame

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 62: Buttons

2.4 RADIUS

RADIUS (Remote Authentication Dial-In User Service) enables server-based authentication of users and terminal devices at a central location in the network. A RADIUS server (AAA system) performs the following tasks:

- Authenticating users or terminal devices logging on.
- Authorizing the logged on users or terminal devices for specific functions or applications.
- Recording transaction data (accounting).

The device performs the role of a RADIUS client. The device transmits the data for the user logging in to the RADIUS server. The RADIUS server compares the login data with the access data stored in its database. If this data matches, the RADIUS server informs the device that the login was successful. In addition, the RADIUS server transmits the user’s authorizations to the device and records the user’s transaction data.

You activate the use of a RADIUS server in the `Security:Authentication List` dialog.

If a user is logging in on the device and the authentication list rule applies here, the device contacts the RADIUS server. In this case, a locally set-up user account on the device is not necessary. If the user identifies himself with a valid user name and password, the RADIUS server authorizes the access to the management functions of the device.

The menu contains the following dialogs:

- RADIUS Global
- RADIUS Authentication Server
- Authentication Statistics

2.4.1 RADIUS Global

This dialog allows you to configure the settings for the communication between the device and the RADIUS servers.

■ RADIUS Configuration

Parameters	Meaning
Max. Number of Retransmits	Defines how often the device resubmits an unanswered request to the RADIUS server before the device sends the request to an alternative RADIUS server. Possible values: ▶ `1..15` (Default setting: `4`)
Timeout [s]	Defines how many seconds the device waits for a response after a request to a RADIUS server before it resubmits the request. Possible values: ▶ `1..30` (Default setting: `5`)
NAS IP Address (Attribute 4)	Defines an IP address that the device transfers to the RADIUS server as attribute 4. Enter the IP address of the device or another freely selectable address. Possible values: ▶ Valid IPv4 address (Default setting: `0.0.0.0`) In many cases, there is a firewall between the device and the RADIUS server. In the Network Address Translation (NAT) in the firewall the original IP address changes, and the RADIUS server receives the translated IP address of the device. The IP address in this field is transferred unchanged by the device across the Network Address Translation (NAT).

Table 63: "Global" dialog, "RADIUS Configuration" frame

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Clear Radius Statistics …	Clears the statistics in the `Security:RADIUS:Authentication Statistics` dialog and the statistics in the `Security:RADIUS:Accounting Statistics` dialog.
Help	Opens the online help.

Table 64: Buttons

2.4.2 RADIUS Authentication Server

To authenticate users or terminal devices, the device contacts a RADIUS authentication server.

The device sends the authentication requests to the primary authentication server. If the primary server fails, the device contacts the first server in the table. If no response comes from this server either, the device contacts the next server in the table.

This dialog allows you to configure up to 8 authentication servers.

■ Table

To change settings click the desired parameter in the table and modify the value.

Parameters	Meaning
Index	Shows a sequential number to which the table entry relates. The device automatically defines this number. Possible values: ▶ `1..8`
Name	Specifies the name of the authentication server. The device automatically specifies the name. You can change the name at any time. Possible values: ▶ 1..32 alphanumeric characters (Default setting: `Default RADIUS Server`)
Address	Specifies the IP address of the authentication server. Possible values: ▶ Valid IPv4 address
UDP Port	Specifies the UDP port of the authentication server. Possible values: ▶ `0..65535` (Default setting: `1812`)
Secret	Enter the password with which the device logs on to the server. You get the password from the server administrator. Possible values: ▶ 1..16 alphanumeric characters

Table 65: "RADIUS Authentication Server" dialog, table

Parameters	Meaning
Primary Server	Specifies the primary authentication server. ▶ `Selected` This server is the primary server. If you select multiple servers, the last server selected will be the primary server. ▶ `Not selected` This server is not the primary server.
Active	Activates/deactivates the connection to the authentication server. Possible values: ▶ `Selected` The connection to the authentication server is activated. ▶ `Not selected` The connection to the authentication server is deactivated.

Table 65: "RADIUS Authentication Server" dialog, table (Cont.)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 66: Buttons

2.4.3 Authentication Statistics

With this dialog you can display statistics for the data packets transfered for the authentication. Each row in the table shows the values for an authentication server.

■ Table

Parameters	Meaning
Name	Name of the authentication server to which the table entry relates.
Address	IP address of the authentication server.
Round Trip Time	Time interval in hundredths of a second between the last response received from the server (Access Reply/Access Challenge) and the corresponding data packet sent (Access Request).
Access Requests	Number of access data packets sent to the server minus the data packets sent repeatedly.
Retransmitted Access Request Packets	Number of access data packets sent repeatedly to the server.
Access Accepts	Number of valid or invalid access data packets received by the server.
Access Rejects	Number of access reject data packets received by the server.
Access Challenges	Number of access challenge data packets received by the server.
Malformed Access Responses	Number of malformed access data packets, including data packets with an invalid length, received by the server.
Bad Authenticators	Number of access data packets with an invalid authenticator received by the server.
Pending Requests	Number of access data packets sent to the server for which the device is still waiting for a response.
Timeouts	Number of access data packets sent to the server for which the device has not received a response.
Unknown Types	Number of access data packets with an unknown data type received by the server.
Packets Dropped	Number of access data packets received by the server that the device has dropped for a different reason.

Table 67: "RADIUS Authentication Statistics" dialog, table

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 68: Buttons

2.5 Pre-login Banner

This dialog gives you the option of displaying a text to users before they login to the device. This text can contain a greeting or instructions for the users.

The device shows this text in the login window of the graphical user interface (GUI) and in the Command Line Interface (CLI). Users logging in with SSH see the text regardless of the client used before or during the login.

To display a text only in the Command Line Interface (CLI), you use the settings in the `Security:Management Access:CLI` dialog.

■ Operation

Parameters	Meaning
Operation	When the function is switched on, the device shows the text specified in the "Banner Text" field on the login screen of the graphical user interface (GUI) and on the CLI start screen. Possible values: ▶ `Off` (default setting) Function is switched off. The text information entered in the "Banner Text" field is kept. ▶ `On` Function switched on.

Table 69: "Pre-login Banner" dialog, "Operation" frame

Banner Text

Parameters	Meaning
Banner Text	Defines the text information that the device displays on the login screen of the graphical user interface (GUI) and on the CLI start screen. Possible values: ▶ Maximum 512 alphanumeric characters ▶ including spaces, tabs, line breaks and the following special characters: !#$%&'()*+,-./:;<=>?@[\\]^_`{}~
Remaining Characters	Shows how many characters are still remaining in the "Banner Text" field for the text information. Possible values: ▶ `512..0`

Table 70: "Pre-login Banner" dialog "Banner Text" frame

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 71: Buttons

3 Time

The device allows you to synchronize the system time in the device and in the network with NTP (Network Time Protocol).

The device is equipped with a buffered hardware clock. This keeps the current time

- if the power supply fails or
- if you disconnect the device from the power supply.

Thus the current time is available to you again, e.g. for log entries, when the device is started.

The hardware clock bridges a power supply downtime of 3 hours. The prerequisite is that the power supply of the device has been connected continually for at least 5 minutes beforehand.

The menu contains the following dialogs:

- Basic Settings
- NTP

3.1 Basic Settings

This dialog provides you with the option of specifying the time zone and other time-related settings independently of the time synchronization protocol.

Configuration

Parameters	Meaning
System Time (UTC)	Displays the current date and time with reference to Universal Time Coordinated (UTC).
System Time	Displays the current date and time with reference to the local time: "System time" = "System time (UTC)" + "Local offset [min]" + "Summer time"
Set Time from PC	The device uses the time on the PC as the system time.
Time Source	Shows the time source from which the device gets the time information. The device automatically selects the available time source with the greatest accuracy. Possible values: ▶ `local` System clock of the device. ▶ `ntp` The NTP client is activated and has synchronized itself.
Local Offset [min]	Defines the difference between the local time and the "system time (UTC)" in minutes: "Local offset [min]" = "System time" − "System time (UTC)" Possible values: ▶ `-780..840` (default value: `60`)
Set Offset from PC	The device determines the time zone on your PC and uses it to calculate the difference between the local time and the "system time (UTC)".

Table 72: "Basic Settings" dialog, "Configuration" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 73: Buttons

3.2 NTP

NTP (Network Time Protocol) is a procedure described in RFC 5905 for time synchronization in the network.

On the basis of a reference time source, NTP defines hierarchy levels for time servers and clients. A hierarchy level is known as a “stratum”. Devices of the 1st level (stratum `1`) synchronize themselves directly with the reference time source and make the time information available to clients of the 2nd level (stratum `2`). A GPS receiver or a radio-controlled clock can serve as the reference time source.

The NTP client in the device evaluates the time information of several servers and adjusts its own clock continuously to attain a high level of accuracy. If you also configure the device as an NTP server, it distributes time information to the clients in the subordinate network segment.

The menu contains the following dialogs:

- Global
- Server
- Multicast groups

3.2.1 Global

In this dialog you determine whether the device functions as an NTP client and server or solely as an NTP client.

- As an NTP client, the device takes the coordinated world time (UTC) from one or more NTP servers in the network.
- As an NTP server, the device distributes the coordinated world time (UTC) to NTP clients in the subordinate network segment. The device takes the coordinated world time from one or more NTP servers in the network if these have been specified.

■ Client only

Parameters	Meaning
Client	Activates/deactivates the NTP client in the device. Possible values: ▶ `On` The NTP client is switched on. The device obtains the time information from one or more NTP servers in the network. ▶ `Off` (default setting) The NTP client is switched off. **Note:** Before you activate the client, deactivate the "Server" function in the "Client and Server" frame.
Mode	Specifies from where the NTP client takes the time information. Possible values: ▶ `unicast` (default setting) The NTP client takes the time information from the unicast responses of the servers that are indicated as active in the `Time:NTP:Server` dialog. ▶ `broadcast` The NTP client takes the time information from the broadcast or multicast messages of the servers that are indicated as active in the `Time:NTP:Multicast Groups` dialog.

Table 74: "Global" dialog, "Client only" frame

The device transmits the time information without authentication in the management VLAN as well as in layer 3 on the IP interfaces set up.

Client and Server

Parameters	Meaning
Server	Activates/deactivates the NTP client and the NTP server in the device. Possible values: ▶ `On` The NTP client and the NTP server are switched on. The NTP client obtains the time information from one or more NTP servers in the network. The NTP server distributes the time information to the NTP clients in the subordinate network segment. ▶ `Off` (default setting) The NTP client and the NTP server are switched off. **Note:** If you switch on the NTP client and the NTP server, the device switches off the "Client" function in the "Client only" frame.
Mode	Specifies in which mode the NTP server works. Possible values: ▶ `client-server` (default setting) With this setting, the device obtains the time information from NTP servers in the network and distributes it to NTP clients in the subordinate network segment. – The NTP client takes the time information from the unicast responses of the servers that are indicated as active in the `Time:NTP:Server` dialog. – The NTP server distributes the time information via unicast to the requesting clients. ▶ `Symmetric` With this setting you can integrate the device in a cluster of redundant NTP servers. The device synchronizes the time information with the other NTP servers in the cluster at intervals of 64 seconds. □ In the `Time:NTP:Server` dialog, indicate the NTP servers participating in the cluster as active. □ Specify a uniform value for the stratum for the NTP servers participating in the cluster.
Stratum	Specifies the hierarchical distance of the device to the referent time source. Possible values: ▶ `1..16` (default setting: `12`) Example: Devices of the 1st level (stratum `1`) synchronize themselves directly with the reference time source and make the time information available to clients of the 2nd level (stratum `2`). The device evaluates this value under the following circumstances: ▶ The NTP server in the device is working in `symmetric` mode. or ▶ The device is using the local system clock as the time source. See "Time Source" field in the `Time:Basic Settings` dialog.

Table 75: "Global" dialog, "Client and Server" frame

The device transmits the time information without authentication in the management VLAN as well as in layer 3 on the IP interfaces set up.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 76: Buttons

3.2.2 Server

In this dialog you specify the NTP servers.

- The NTP client of the device obtains the time information from the unicast responses of the servers specified here.
- If the NTP server of the device is working in `symmetric` mode, you specify the servers participating in the cluster here.

■ Table

Parameters	Meaning
Index	Shows a sequential number to which the table entry relates. Possible values: ▶ `1..4` The device automatically defines this number. When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap.
Address	Specifies the IP address of the NTP server. Possible values: ▶ Valid IPv4 address (default setting: `0.0.0.0`)
Port	Defines the UDP Port on which the NTP server provides the time information. Possible values: ▶ `1..65535` (default setting: `123`) Exception: Port `2222` is reserved for internal functions.
Status	Displays the synchronization status. Possible values: ▶ `disabled` No server available. ▶ `notSynchronized` The server is available. The server itself is not synchronized. ▶ `notResponding` The server is available. The device does not receive time information. ▶ `synchronizing` The server is available. The device receives time information. ▶ `synchronized` The server is available. The device has synchronized its clock with the server. ▶ `genericError` Device-internal error.

Table 77: "Server" dialog, table

Parameters	Meaning
Active	Activates/deactivates the connection to the NTP server. Possible values: ▶ `not selected` The connection to the NTP server is deactivated. ▶ `selected` The connection to the NTP server is activated. – The NTP client of the device obtains the time information from the unicast responses of this server. – This server participates in a cluster if the NTP server of the device is working in `symmetric` mode.

Table 77: "Server" dialog, table (Cont.)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 78: Buttons

3.2.3 Multicast groups

In this dialog you define the broadcast and multicast addresses.

In broadcast mode, the NTP client of the device obtains the time information from broadcast or multicast messages from the addresses defined here.

■ Table

Parameters	Meaning
Index	Shows a sequential number to which the table entry relates. Possible values: ▶ `1..4` The device automatically defines this number. When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap.
Address	Specifies the IP address of the broadcast or multicast. Possible values: ▶ Valid IPv4 address (default setting: `0.0.0.0`)
Port	Defines the UDP Port on which the broadcast or multicast provides the time information. Possible values: ▶ `1..65535` (default setting: `123`) Exception: Port `2222` is reserved for internal functions.
Status	Displays the synchronization status. Possible values: ▶ `disabled` No server available. ▶ `notSynchronized` The server is available. The server itself is not synchronized. ▶ `notResponding` The server is available. The device does not receive time information. ▶ `synchronizing` The server is available. The device receives time information. ▶ `synchronized` The server is available. The device has synchronized its clock with the server. ▶ `genericError` Device-internal error.

Table 79: "Multicast Groups" dialog, table

Parameters	Meaning
Active	Activates/deactivates the connection between the device and the broadcast or multicast server. Possible values: ▶ `not selected` The connection to the broadcast or multicast is deactivated. ▶ `selected` The connection to the broadcast or multicast is activated. The NTP client of the device obtains the time information from the broadcast or multicast messages of this IP address.

Table 79: "Multicast Groups" dialog, table (Cont.)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 80: Buttons

4 Network Security

The device has comprehensive configuration options for protecting individual devices and complex networks against undesired or even dangerous network traffic.

It also provides the option to automatically switch addresses between different networks (Network Address Translation, NAT). For example, you can hide multiple devices behind one IP address or automatically divert data packets to other devices.
The packet filter is one of the central elements of the security function. This allows you to selectively filter and forward data packets. Here the device considers the state of the connection, thus also detecting devices that belong to a specific connection (Stateful Packet Inspection).

The device can perform the following with data packets

- ▶ Accept: The device forwards the data packet to its destination.
- ▶ Reject: The device discards the data packet and informs the sender.
- ▶ Drop: The device discards the data packet without informing the sender.

The device applies the complete packet filter and NAT function only to routed data traffic on layers 3-7.
In addition to the packet filter, there is the option to filter incoming data traffic using Access Control Lists (ACL). Here the device combines complete sets of rules into ACLs and assigns these to physical ports or VLANs. The filter criteria can be on the Ethernet or IP/UDP/TCP level.

The network security area also provides protection against invalid or fake data traffic that aims to bring down specific services or devices (Denial of Service, DoS).

A data packet passes through the network security rules in the device in the following sequence:

- ▶ DoS … if `permit` or `accept`, then progress to the next rule
- ▶ ACL … if `permit` or `accept`, then progress to the next rule
- ▶ NAT (if rule present)
- ▶ Routing … if `permit` or `accept`, then progress to the next rule
- ▶ Packet Filters

The menu contains the following dialogs:

- Overview
- Packet Filters
- NAT Global
- 1:1 NAT
- Destination NAT
- Masquerading NAT
- Double NAT
- DoS
- Access Control Lists

4.1 Overview

This dialog allows you to display the network security rules.

■ Parameter

Parameter	Meaning
Port/VLAN	Specifies whether VLAN- or port-based rules are displayed. Possible values: ▶ All (state on delivery) Displays VLAN- and port-based rules.
Layer3	Displays Layer 3 rules in the overview.
1:1 NAT	Displays 1:1 NAT rules in the overview.
Destination NAT	Displays Destination NAT rules in the overview.
Masquerading NAT	Displays Masquerading NAT rules in the overview.
Double NAT	Displays Double NAT rules in the overview.
DoS	Displays Denial-of-Service rules in the overview.
ACL	Displays ACL rules in the overview.
All	Selects the adjacent checkboxes. The related rules are visible in the overview.
None	Removes the selections in the adjacent checkboxes. The overview does not display any rules.

Table 81: "Overview" dialog, parameters

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 82: Buttons

4.2 Packet Filters

A packet filter provides state-oriented evaluation of data traffic and allows selective filtering and forwarding of undesired data traffic. The device only uses packet filters on routed data traffic. It also only uses rules when you have assigned them to a routing interface.

When the device receives a data packet to be routed, it works through the packet filter rules sequentially until the first rule applies to the data packet. The subsequent rules are ignored (“first match wins”).

If none of the configured rules applies, the packet filter has a standard rule, which it then applies. You have the option to configure this standard rule:

- `accept`: The device forwards the data packet to its destination.
- `reject`: The device discards the data packet and informs the sender.
- `drop`: The device discards the data packet without informing the sender.

Note: If you have not entered any settings in the firewall yet, the standard rule `accept` overrules the state on delivery `drop`. Therefore all data traffic can pass unhindered until you have configured one or more interfaces in the firewall.

The packet filter adheres to a two-level concept in transferring the rules to the packet filter tables. Here you have the option of changing any number of packet filter rules and other parameters of the packet filter and transferring them to the device using the "Set" button. Only after you press the “Commit Changes” button in the `Network Security:Packet Filter:Global` dialog are these changes transferred to the rule tables of the packet filter.

With this menu you can define the rules for the packet filter.

Note: As soon as the device activates a rule, it is not possible to set up a new connection.

The menu contains the following dialogs:

- Global
- Rule
- Assignment
- Overview

4.2.1 Global

With this dialog you can enter the global settings for the packet filter.

■ Configuration

Parameter	Meaning
Max. number of allowed rules for L3 firewalling	Shows the maximum number of allowed firewall rules for data packets.
Default Policy	Defines how the firewall handles data packets if no rule applies. Possible values: ▶ `accept` The device accepts all incoming data packets. ▶ `drop` (state on delivery) The device discards all incoming data packets. ▶ `reject` The device discards all incoming data packet and sends an ICMP Admin Prohibited message to the sender.

Table 83: "Global" dialog, "Configuration" frame

■ Information

Parameter	Meaning
Uncommitted Changes present	Shows whether the packet filter contains changes that are not saved in the volatile memory of the device yet.

Table 84: "Global" dialog, "Information" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Commit Changes	Applies the changes after they are saved to the corresponding ports.
Help	Opens the online help.

Table 85: Buttons

4.2.2 Rule

This dialog allows you to configure rules for the packet filter. You can assign the rules defined here to the desired ports in the `Network Security:Packet Filter:Assignment` dialog.

■ Table

Parameter	Meaning
Rule Index	Shows the sequential number of the rule. The device automatically defines this number.
Description	Defines a name or description for the rule.
Source Address	Defines the source address for which this rule applies. Possible values: ▶ valid IPv4 address and netmask in CIDR notation ▶ `any` (state on delivery) The rule applies to all source addresses.
Destination Address	Defines the destination address for which this rule applies. Possible values: ▶ valid IPv4 address and netmask in CIDR notation ▶ `any` (state on delivery) The rule applies to all destination addresses.

Table 86: "Rule" dialog, table (section 1 of 5)

Parameter	Meaning
Protocol	Shows the protocol via which the device receives the data packet. Possible values: ▶ `any` (state on delivery) The rule applies to data packets of all protocols. ▶ `icmp` The rule applies to ICMP data packets (Internet Control Message Protocol). ▶ `igmp` The rule applies to IGMP data packets (Internet Group Management Protocol). ▶ `ipip` The rule applies to data packets that the device receives via an IPIP tunnel. ▶ `tcp` The rule applies to TCP data packets (Transmission Control Protocol). ▶ `udp` The rules applies to UDP data packets (User Datagram Protocol). ▶ `esp` The rule applies to the data packets that the device receives with Encapsulated Security Payload. ▶ `ah` The rule applies to data packets that the device receives via the Authentication Header protocol. ▶ `icmpv6` The rule applies to ICMPv6 data packets (Internet Control Message Protocol Version 6).
Source Port	Defines the source port from which the device considers data packets for this rule. You can only make these settings if you are using these rules for a protocol that considers ports. Possible values: ▶ `any` (state on delivery) The rule applies to data packets of all source ports. ▶ <Port number> The rule applies to the specified port, e.g. `10`. ▶ <Port number range> The rule applies to the specified range, e.g. `8-25`. Separator: hyphen ▶ <List of individual ports> The rule applies to the specified ports, e.g. `1,7,9,65` Separator: comma ▶ A combination of the options named above, e.g. `1,7-13,65.` The system limits the number of port entries to 15, whereby a single number stands for 1 port and two numbers stand for a port range. Thus, in the above example, 4 of 15 numbers are being used.

Table 86: "Rule" dialog, table (section 2 of 5)

Parameter	Meaning
Destination Port	Defines the destination port for which the device considers data packets for this rule. You can only make these settings if you are using these rules for a protocol that considers ports. Possible values: ▶ any (state on delivery) The rule applies to data packets of all destination ports. ▶ <Port number> The rule applies to the specified port, e.g. 10. ▶ <Port number range> The rule applies to the specified range, e.g. 8-25. Separator: hyphen ▶ <List of individual ports> The rule applies to the specified ports, e.g. 1,7,9,65 Separator: comma ▶ A combination of the options named above, e.g. 1,7-13,65. The system limits the number of port entries to 15, whereby a single number stands for 1 port and two numbers stand for a port range. Thus, in the above example, 4 of 15 numbers are being used.

Table 86: "Rule" dialog, table (section 3 of 5)

Parameter	Meaning
Parameter	Defines additional parameters for this rule. Enter the parameters using the notation `<key>=<value>`. If you enter several parameters, separate them with commas. If you enter several values, separate them with dashes. Some keys are only valid if you use a certain protocol. Exception: The values `macand state` are valid independent from the protocol. You also can combine general rules and protocol specific rules. Possible values: ▶ `none` (state of delivery) No additional parameters for this rule defined. ▶ `mac=de:ad:de:ad:be:ef` This rule applies exclusively for packets with the source MAC address de:ad:de:ad:be:ef. ▶ `state=new` This rule applies exclusively for packets belonging to a new connection. ▶ `state=rel` This rule applies exclusively for packets belonging to a new connection which is related to an existing connection (e.g. an FTP data connection, after you have established the control connection). ▶ `state=est` This rule applies exclusively for packets belonging to an already existing connection. ▶ `state=new|rel|est` This rule applies exclusively for packets belonging to a new, a relative or an already existing connection. ▶ `type=<number>` This rule applies exclusively for packets of a certain ICMP type. Enter exactly one value for <number>. Possible values: `0..255` (Meaning of these values see RFC 792) ▶ `code=<number>` This rule applies exclusively for packets of a certain ICMP code. Enter exactly one value for <number>. Possible values: `0..255` (Meaning of these values see RFC 792) ▶ `flags=<value>` This rule applies exclusively for packets having certain flags set. Possible values: `syn|ack|fin|psh|rst`. ▶ `flags=syn` This rule applies exclusively for packets having the `syn` flag set. ▶ `flags=syn|ack|fin|rst` This rule applies exclusively for packets having the `syn`, `ack`, `fin` or `rst` flag set. ▶ `mac=de:ad:de:ad:be:ef,state=new|rel,flags=syn` This rule applies exclusively for packets with the source MAC address `de:ad:de:ad:be:ef`, belonging to a new or relative connection and having the `syn` flag set.

Table 86: "Rule" dialog, table (section 4 of 5)

Parameter	Meaning
Action	Defines how the device handles received data packets. Possible values: ▶ `accept` (state on delivery) The device accepts the data packets. ▶ `drop` The device drops the data packets. ▶ `reject` The device rejects the data packets.
Log	Defines whether the device creates log entries when it uses the rule for data packets. Possible values: ▶ `selected` Logging is activated. ▶ `not selected` (state on delivery) Logging is deactivated.
Trap	Defines whether the device sends an SNMP message (trap) when it uses the rule for data packets. Possible values: ▶ `selected` The device sends a trap. ▶ `not selected` (state on delivery) The device does not send a trap.
Active	Activates/deactivates the rule. Possible values: ▶ `selected` (state on delivery) The rule is activated. ▶ `not selected` The rule is deactivated.

Table 86: "Rule" dialog, table (section 5 of 5)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 87: Buttons

4.2.3 Assignment

With this dialog you can assign the packet filter rules for individual ports. To create a new rule for an interface, you first set up the rule in the `Network Security:Packet Filter:Rule` dialog.

Note: You have to set up a routing interface and give it an IP address before you can assign rules to it. You can enter these settings in the `Routing:Interfaces:Configuration` dialog.

■ Information

Parameter	Meaning
Assignment Count	Shows how many rules are active for the ports.
Uncommitted Changes present	Shows whether the packet filter contains changes that are not saved in the volatile memory of the device yet.

Table 88: "Assignment" dialog, "Information" frame

Table

Parameter	Meaning
Description	Shows the name or description of the rule. You define the description in the `Network Security:Packet Filter:Rule` dialog.
Rule Index	Shows the sequential number of the rule. You define the index by clicking on the "Assign" button.
Port	Shows the interface on which the device uses the rule. You define the interface by clicking on the "Assign" button. The device only shows ports on which routing is activated.
Direction	Shows the data packets to which the rule applies. You define the value by clicking on the "Assign" button. Possible values: ▶ `ingress` The rule applies to data packets that the interface receives. ▶ `egress` The rule applies to data packets that the interface sends. ▶ `both` The rule applies to data packets that the interface sends and receives.
Priority	Defines the priority of the rule.
Active	Activates/deactivates the rule. Possible values: ▶ `selected` (state on delivery) The rule is activated. ▶ `not selected` The rule is deactivated.

Table 89: "Assignment" dialog, table

Port

Parameter	Meaning
Port	Defines which rules the table displays. Possible values: ▶ `All` The table shows all the rules. ▶ <Port number> The table only shows the rules that apply for the selected port.

Table 90: "Assignment" dialog, "Port" field

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Assign	Assign a rule to an interface.
Remove	Removes the selected table entry.
Commit Changes	Applies the changes after they are saved to the corresponding ports.
Help	Opens the online help.

Table 91: Buttons

4.2.4 Overview

This dialog gives you an overview of the defined packet filter rules.

■ Table

Parameter	Meaning
Description	Shows the name or description of the rule. You define the description in the `Network Security:Packet Filter:Rule` dialog.
Rule Index	Shows the sequential number of the rule.
Port	Shows the interface on which the device uses the rule.
Direction	Shows the data packets to which the rule applies. Possible values: ▶ `ingress` The rule applies to data packets that the interface receives. ▶ egress The rule applies to data packets that the interface sends. ▶ `both` The rule applies to data packets that the interface sends and receives.
Priority	Shows the priority of the rule.
Source Address	Shows the source address for which this rule applies. Possible values: ▶ valid IPv4 address and netmask in CIDR notation ▶ `any` The rule applies to all source addresses.
Source Port	Shows the source port for which this rule applies. Possible values: ▶ `any` (state on delivery) The rule applies to data packets of all source ports. ▶ <Port number> The rule applies to the specified port, e.g. `10`. ▶ <Port number range> The rule applies to the specified range, e.g. `8-25`. Separator: hyphen ▶ <List of individual ports> The rule applies to the specified ports, e.g. `1,7,9,65` Separator: comma ▶ A combination of the options named above, e.g. `1,7-13,65.` The system limits the number of port entries to 15, whereby a single number stands for 1 port and two numbers stand for a port range. Thus, in the above example, 4 of 15 numbers are being used.

Table 92: "Overview" dialog, table (section 1 of 4)

Parameter	Meaning
Destination Address	Shows the destination address for which this rule applies. Possible values: ▶ valid IPv4 address and netmask in CIDR notation ▶ any The rule applies to all destination addresses.
Destination Port	Shows the destination port for which this rule applies. Possible values: ▶ any (state on delivery) The rule applies to data packets of all destination ports. ▶ <Port number> The rule applies to the specified port, e.g. 10. ▶ <Port number range> The rule applies to the specified range, e.g. 8-25. Separator: hyphen ▶ <List of individual ports> The rule applies to the specified ports, e.g. 1,7,9,65 Separator: comma ▶ A combination of the options named above, e.g. 1,7-13,65. The system limits the number of port entries to 15, whereby a single number stands for 1 port and two numbers stand for a port range. Thus, in the above example, 4 of 15 numbers are being used.
Protocol	Shows the protocol via which the device receives the data packet. Possible values: ▶ any (state on delivery) The rule applies to data packets of all protocols. ▶ icmp The rule applies to ICMP data packets (Internet Control Message Protocol). ▶ igmp The rule applies to IGMP data packets (Internet Group Management Protocol). ▶ ipip The rule applies to data packets that the device receives via an IPIP tunnel. ▶ tcp The rule applies to TCP data packets (Transmission Control Protocol). ▶ udp The rules applies to UDP data packets (User Datagram Protocol). ▶ esp The rule applies to the data packets that the device receives with Encapsulated Security Payload. ▶ ah The rule applies to data packets that the device receives via the Authentication Header protocol. ▶ icmpv6 The rule applies to ICMPv6 data packets (Internet Control Message Protocol Version 6).

Table 92: "Overview" dialog, table (section 2 of 4)

Parameter	Meaning
Parameter	Shows additional parameters for this rule. Possible values: ▶ `none` (state of delivery) No additional parameters for this rule defined. ▶ `mac=de:ad:de:ad:be:ef` This rule applies exclusively for packets with the source MAC address de:ad:de:ad:be:ef. ▶ `state=new` This rule applies exclusively for packets belonging to a new connection. ▶ `state=rel` This rule applies exclusively for packets belonging to a new connection which is related to an existing connection (e.g. an FTP data connection, after you have established the control connection). ▶ `state=est` This rule applies exclusively for packets belonging to an already existing connection. ▶ `state=new|rel|est` This rule applies exclusively for packets belonging to a new, a relative or an already existing connection. ▶ `type=<number>` This rule applies exclusively for packets of a certain ICMP type. Enter exactly one value for <number>. Possible values: `0..255` (Meaning of these values see RFC 792) ▶ `code=<number>` This rule applies exclusively for packets of a certain ICMP code. Enter exactly one value for <number>. Possible values: `0..255` (Meaning of these values see RFC 792) ▶ `flags=<value>` This rule applies exclusively for packets having certain flags set. Possible values: `syn|ack|fin|psh|rst`. ▶ `flags=syn` This rule applies exclusively for packets having the `syn` flag set. ▶ `flags=syn|ack|fin|rst` This rule applies exclusively for packets having the `syn`, `ack`, `fin` or `rst` flag set. ▶ `mac=de:ad:de:ad:be:ef,state=new|rel,flags=syn` This rule applies exclusively for packets with the source MAC address `de:ad:de:ad:be:ef`, belonging to a new or relative connection and having the `syn` flag set.
Action	Shows how the device handles received data packets. Possible values: ▶ `accept` The device accepts the data packets. ▶ `drop` The device drops the data packets. ▶ `reject` The device rejects the data packets.

Table 92: "Overview" dialog, table (section 3 of 4)

Parameter	Meaning
Log	Shows whether the device creates log entries when it uses the rule for data packets. Possible values: ▶ `selected` Logging is activated. ▶ `not selected` Logging is deactivated.
Trap	Shows whether the device sends an SNMP message (trap) when it uses the rule for data packets. Possible values: ▶ `selected` The device sends a trap. ▶ `not selected` (state on delivery) The device does not send a trap.

Table 92: "Overview" dialog, table (section 4 of 4)

Port

Parameter	Meaning
Port	Defines which rules the table displays. Possible values: ▶ `All` The table shows all the rules. ▶ <Port number> The table only shows the rules that apply for the selected port.

Table 93: "Assignment" dialog, "Port" field

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 94: Buttons

4.3 NAT Global

This dialog shows the maximum number of rules allowed for the different NAT types, and whether unwritten changes exist for these areas.

Information

Parameter	Meaning
Maximum Rules Destination NAT	Shows the maximum number of allowed Destination NAT rules.
Maximum Rules 1:1 NAT	Shows the maximum number of allowed 1:1 NAT rules.
Maximum Rules Masquerading NAT	Shows the maximum number of allowed Masquerading NAT rules.
Maximum Rules Double NAT	Shows the maximum number of allowed Double NAT rules.
Destination NAT Pending Actions	Shows whether there are unwritten changes for the Destination NAT settings.
1:1 NAT Pending Actions	Shows whether there are unwritten changes for the 1:1 NAT settings.
Masquerading NAT Pending Actions	Shows whether there are unwritten changes for the Masquerading NAT settings.
Double NAT Pending Actions	Shows whether there are unwritten changes in the Double NAT rules.

Table 95: "Global" dialog, "Information" frame

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Commit Changes	Applies the changes after they are saved to the corresponding ports.
Help	Opens the online help.

Table 96: Buttons

4.4 1:1 NAT

This dialog allows you to enter the rule settings for the 1:1 address translation.

With 1:1 NAT, the device operates as a router and allocates an additional IP address in the external network for a terminal device in the internal network. In addition, as a proxy the device answers the ARP queries for the additional IP address in the external network. For sent data packets, the device replaces the internal source IP address of the terminal device with its external IP address. For received data packets, the device replaces the external destination IP address with the internal IP address.

Note: As soon as the device activates a rule, it is not possible to set up a new connection.

The menu contains the following dialog:

- Rule

4.4.1 Rule

This dialog allows you to enter, edit or delete the rules for the 1:1 address translation. You can add up to 255 entries.

■ Table

Parameter	Meaning
Index	Shows the sequential number of the rule. The device automatically defines this number.
Rule Name	Defines the name of the rule. Alternatively, you can define the name using the "Create" button.
Priority	Defines the priority of the rule.
Ingress Interface	Defines the interface to which the external network is connected. Possible values: ▶ `No port` (state on delivery) No interface selected. ▶ <Port number> The device only shows ports on which routing is activated.
Destination Address	The existing target IP address of the connection. Possible values: ▶ valid IPv4 address and netmask in CIDR notation ▶ `any` The rule applies to all destination addresses.
Egress Interface	Defines the interface to which the internal interface is connected. Possible values: ▶ `No port` (state on delivery) No interface defined. ▶ <Port number> The device only shows ports on which routing is activated.
New Destination Address	Defines the new destination IP address of the connnection. Possible values: ▶ valid IPv4 address and netmask in CIDR notation ▶ `any` The rule applies to all destination addresses.

Table 97: "Rule" dialog, table

Parameter	Meaning
Trap	Defines whether the device sends an SNMP message (trap) when it uses the rule for data packets. Possible values: ▶ `selected` The device sends a trap. ▶ `not selected` (state on delivery) The device does not send a trap.
Log	Defines whether the device creates log entries when it uses the rule for data packets. Possible values: ▶ `selected` Logging is activated. ▶ `not selected` (state on delivery) Logging is deactivated.
Active	Activates/deactivates the rule. Possible values: ▶ `selected` The rule is activated. ▶ `not selected` (state on delivery) The rule is deactivated.

Table 97: "Rule" dialog, table (Cont.)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Set and back	Transfers the changes to the volatile memory (`RAM`) of the device and goes back to the previous dialog.
Back	Displays the previous dialog again. Changes are lost.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 98: Buttons

4.5 Destination NAT

This menu allows you to configure the rules for the Destination NAT procedure. In this procedure, the device replaces both the source and target IP addresses for a continuous connection.
The application cases for this procedure are Port Forwarding and Redirect (changing the IP address).

Note: As soon as the device activates a rule, it is not possible to set up a new connection.

The menu contains the following dialogs:

- Rule
- Assignment
- Overview

4.5.1 Rule

This dialog allows you to configure, delete and edit rules for the Destination NAT procedure. You can define up to 255 rules.

In the `Network Security:Destination NAT:Mapping` dialog, the rules created here are assigned to specific ports. These rules become effective when they are assigned to an interface.

■ Table

Parameter	Meaning
Index	Shows the sequential number of the rule. The device automatically defines this number
Rule Name	Defines the name of the rule. Alternatively, you can define the name using the "Create" button.
Source Address	Restricts Destination NAT to the source addresses defined here. Possible values: ▶ valid IPv4 address or area and netmask in CIDR notation ▶ `any` No restriction effective.
Source Port	Restricts the Destination NAT procedure to specific source port numbers. The value `any` means no restriction. You have the option to configure individual ports or areas. The system limits the number of port entries to 15, whereby a single number stands for 1 port and two numbers stand for a port range. If you enter `1,7-13,65` here, for example, you are using 4 of 15 numbers. You have the option of configuring a port exclusively in connection with the TCP or UDP protocols.
Destination Address	The original destination address of the connection. Possible values: ▶ `any` The rule applies to the data packets of all connections. ▶ Up to 20 numeric characters, as well as dots and slashes (e.g. `192.169.2.6`) in the form of an IP address or a CIDR mask

Table 99: "Rule" dialog, table (section 1 of 3)

Parameter	Meaning
Destination Port	The original destination port of the connection. Possible values: ▶ `any` The rule applies to the data packets of all ports. ▶ Numeric characters for individual ports or port areas. The system limits the number of port entries to 15, whereby a single number stands for 1 port and two numbers stand for a port range. If you enter `1,7-13,65` here, for example, you are using 4 of 15 numbers.
New Destination Address	The new destination address of the connection to which the data packets are forwarded. Possible values: ▶ Up to 20 numeric characters, as well as dots and slashes (e.g. `192.169.2.6`) in the form of an IP address or a CIDR mask
New Destination Port	The new destination port of the connection to which the data packets are forwarded. Possible values: ▶ Numeric characters, e.g. `19`
Protocol	Defines the protocol for which this rule applies. Possible values: ▶ `any` The rule applies to data packets of all protocols. ▶ `tcp` The rule applies to TCP data packets (Transmission Control Protocol). ▶ `udp` The rules applies to UDP data packets (User Datagram Protocol).
Log	Defines whether the device creates log entries when it uses the rule for data packets. Possible values: ▶ `selected` Logging is activated. ▶ `not selected` (state on delivery) Logging is deactivated.
Trap	Defines whether the device sends an SNMP message (trap) when it uses the rule for data packets. Possible values: ▶ `selected` The device sends a trap. ▶ `not selected` (state on delivery) The device does not send a trap.

Table 99: "Rule" dialog, table (section 2 of 3)

Parameter	Meaning
Active	Activates/deactivates the rule. Possible values: ▶ `selected` The rule is activated. ▶ `not selected` (state on delivery) The rule is deactivated.

Table 99: "Rule" dialog, table (section 3 of 3)

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Set and back	Transfers the changes to the volatile memory (`RAM`) of the device and goes back to the previous dialog.
Back	Displays the previous dialog again. Changes are lost.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 100: Buttons

4.5.2 Assignment

With this dialog you can assign Destination NAT rules to individual ports.

You create new rules for an interface in the Network Security:Destination NAT:Rule dialog.

■ Table

Parameter	Meaning
Port	Shows the number of the interface on which the device uses the rule.
Rule Index	Shows the sequential number of the rule.
Rule Name	Shows the name of the rule.
Direction	Shows the data packets to which the rule applies. You define the value by clicking on the "Assign" button. Possible values: ▶ ingress The rule applies to data packets that the interface receives.
Priority	Displays the priority of the entry.
Active	Activates/deactivates the rule. Possible values: ▶ selected (state on delivery) The rule is activated. ▶ not selected The rule is deactivated.

Table 101: "Assignment" dialog, table

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Assign	Assign a rule to an interface.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 102: Buttons

4.5.3 Overview

This dialog gives you an overview of all the Destination NAT rules.

■ Table

Parameter	Meaning
Port	Shows the number of the interface on which the device uses the rule.
Rule Index	Shows the sequential number of the rule.
Rule Name	Shows the name of the rule.
Destination Address	Shows the existing destination IP address of the connection. Possible values: ▶ Up to 20 numeric characters, as well as dots and slashes (e.g. `192.169.2.6`) in the form of an IP address or a CIDR mask
New Destination Address	Shows the new destination IP address of the connection. Possible values: ▶ Up to 20 numeric characters, as well as dots and slashes (e.g. `192.169.2.6`) in the form of an IP address or a CIDR mask
Trap	Shows whether the device sends an SNMP message (trap) when it uses the rule for data packets. Possible values: ▶ `selected` The device sends a trap. ▶ `not selected` (state on delivery) The device does not send a trap.
Log	Shows whether the device creates log entries when it uses the rule for data packets. Possible values: ▶ `selected` Logging is activated. ▶ `not selected` (state on delivery) Logging is deactivated.
Direction	Shows the data packets to which the rule applies. Possible values: ▶ `ingress` The rule applies to data packets that the interface receives.
Priority	Displays the priority of this rule.

Table 103:"Overview" dialog, table

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 104: Buttons

4.6 Masquerading NAT

Note: As soon as the device activates a rule, it is not possible to set up a new connection.

The menu contains the following dialogs:

- ▶ Rule
- ▶ Assignment
- ▶ Overview

4.6.1 Rule

With this dialog you can configure the rules for the Masquerading. Masquerading is a procedure in which the device maps any number of IP addresses onto a single IP address (N:1 NAT). Specifically, this means that any number of hosts can use the IP address of the router for the external communication.

The prerequisite is an egress interface whose address is then used as the source address for all the external connections.

You can set up up to 128 entries Masquerading rules. To assign these rules to the corresponding interfaces, select the `Network Security:Masquerading NAT:Mapping` dialog. After the assignment, the rules become effective.

■ Table

Parameter	Meaning
Index	Shows the sequential number of the rule. The device automatically defines this number.
Rule Name	Defines the name of the rule. Alternatively, you can define the name using the "Create" button.
Source Address	Restricts the Masquerading to specific source addresses. The value `any` means no restriction. The source address can be an individual address or a range (CIDR notation).
Source Port	Restricts the Masquerading to specific source port numbers. The value `any` means no restriction. You have the option to configure individual ports or areas. The system limits the number of port entries to 15, whereby a single number stands for 1 port and two numbers stand for a port range. If you enter `1,7-13,65` here, for example, you are using 4 of 15 numbers. You have the option of configuring a port exclusively in connection with the TCP or UDP protocols.

Table 105: "Rule" dialog, table

Parameter	Meaning
Protocol	Shows the protocol via which the device receives the data packet. Possible values: ▶ `any` The rule applies to the data packets of all protocols. ▶ `tcp` This rule applies to TCP data packets (Transmission Control Protocol). ▶ `udp` This rules applies to UDP data packets (User Datagram Protocol).
Log	Defines whether the device creates log entries when it uses the rule for data packets. Possible values: ▶ `selected` Logging is activated. ▶ `not selected` (state on delivery) Logging is deactivated.
Trap	Defines whether the device sends an SNMP message (trap) when it uses the rule for data packets. Possible values: ▶ `selected` The device sends a trap. ▶ `not selected` (state on delivery) The device does not send a trap.
Active	Activates/deactivates the rule. Possible values: ▶ `selected` The rule is activated. ▶ `not selected` (state on delivery) The rule is deactivated.

Table 105:"Rule" dialog, table (Cont.)

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Set and back	Transfers the changes to the volatile memory (`RAM`) of the device and goes back to the previous dialog.
Back	Displays the previous dialog again. Changes are lost.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 106: Buttons

4.6.2 Assignment

With this dialog you can assign Masquerading rules to individual ports. In the `Network Security:Masquerading NAT:Rule` dialog, new Masquerading rules can be created.

Table

Parameter	Meaning
Port	Shows the number of the interface on which the device uses the rule. You define the interface by clicking on the "Assign" button. The device only shows ports on which routing is activated.
Rule Index	Shows the sequential number of the rule.
Rule Name	Shows the name of the rule.
Direction	Shows the data packets to which the rule applies. You define the value by clicking on the "Assign" button. Possible values: ▶ egress The rule applies to data packets that the interface sends.
Priority	Defines the priority of the rule.
Active	Activates/deactivates the rule. Possible values: ▶ `selected` (state on delivery) The rule is activated. ▶ `not selected` The rule is deactivated.

Table 107: "Assignment" dialog, table

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Assign	Assign a rule to an interface.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 108: Buttons

4.6.3 Overview

This dialog gives you an overview of the existing Masquerading rules.

■ Table

Parameter	Meaning
Port	Shows the number of the interface on which the device uses the rule.
Rule Index	Shows the sequential number of the rule.
Rule Name	Shows the name of the rule.
Trap	Shows whether the device sends an SNMP message (trap) when it uses the rule for data packets. Possible values: ▶ `selected` The device sends a trap. ▶ `not selected` (state on delivery) The device does not send a trap.
Log	Shows whether the device creates log entries when it uses the rule for data packets. Possible values: ▶ `selected` Logging is activated. ▶ `not selected` (state on delivery) Logging is deactivated.
Direction	Shows the data packets to which the rule applies. Possible values: ▶ egress The rule applies to data packets that the interface sends.
Priority	Displays the priority of the rule.

Table 109: "Overview" dialog, table

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 110: Buttons

4.7 Double NAT

This dialog allows you to set up rules for the Double NAT procedure and assign them to individual ports. In the Double NAT procedure, the device replaces both the source and target addresses for data packets to be forwarded. This is useful if two subscribers want to communicate with each other who are active in different networks and have different IP addresses within these networks than can be seen from outside. In this case, the subscribers each have an external and an internal IP address, which the device switches with each other.

Note: As soon as the device activates a rule, it is not possible to set up a new connection.

The menu contains the following dialogs:

- Rule
- Assignment
- Overview

4.7.1 Rule

This dialog allows you to define up to 255 Double NAT rules for incoming and outgoing connections. In the `Network Security:Double NAT:Mapping` dialog, a rule can be assigned to an interface. The rules become effective when you assign them to an interface.

■ Table

Parameter	Meaning
Index	Shows the sequential number of the rule. The device automatically defines this number.
Rule Name	Defines the name of the rule. Alternatively, you can define the name using the "Create" button.
Local Internal IP Address	Defines the local internal IP address of the first subscriber. Possible values: ▶ Up to 20 numeric characters, as well as dots and slashes (e.g. `192.169.2.6`) in the form of an IP address
Local External IP Address	Defines the local external IP address of the first subscriber into which the device translates the internal local address of the first subscriber. Possible values: ▶ Up to 20 numeric characters, as well as dots and slashes (e.g. `192.169.2.6`) in the form of an IP address
Remote Internal IP Address	Defines the remote internal IP address of the second subscriber. Possible values: ▶ Up to 20 numeric characters, as well as dots and slashes (e.g. `192.169.2.6`) in the form of an IP address
Remote External IP Address	Defines the remote external IP address into which the device translates the internal address of the second subscriber. Possible values: ▶ Up to 20 numeric characters, as well as dots and slashes (e.g. `192.169.2.6`) in the form of an IP address
Log	Defines whether the device creates log entries when it uses the rule for data packets. Possible values: ▶ `selected` Logging is activated. ▶ `not selected` (state on delivery) Logging is deactivated.

Table 111: "Rule" dialog, table

Parameter	Meaning
Trap	Defines whether the device sends an SNMP message (trap) when it uses the rule for data packets. Possible values: ▶ `selected` The device sends a trap. ▶ `not selected` (state on delivery) The device does not send a trap.
Active	Activates/deactivates the rule. Possible values: ▶ `selected` The rule is activated. ▶ `not selected` (state on delivery) The rule is deactivated.

Table 111: "Rule" dialog, table (Cont.)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Set and back	Transfers the changes to the volatile memory (`RAM`) of the device and goes back to the previous dialog.
Back	Displays the previous dialog again. Changes are lost.
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 112: Buttons

4.7.2 Assignment

With this dialog you can assign the Double NAT rules to specific ports. In the `Network Security:Double NAT:Rule` dialog, you can create Double Nat rules.

■ Table

Parameter	Meaning
Port	Shows the number of the interface on which the device uses the rule. You define the interface by clicking on the "Assign" button. The device only shows ports on which routing is activated.
Rule Index	Shows the sequential number of the rule.
Rule Name	Shows the name of the rule.
Direction	Shows the data packets to which the rule applies. You define the value by clicking on the "Assign" button. Possible values: ▶ `ingress` The rule applies to data packets that the interface receives. ▶ `egress` The rule applies to data packets that the interface sends. ▶ `both` The rule applies to data packets that the interface sends and receives.
Priority	Defines the priority of the rule.
Active	Activates/deactivates the rule. Possible values: ▶ `selected` (state on delivery) The rule is activated. ▶ `not selected` The rule is deactivated.

Table 113: "Assignment" dialog, table

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Assign	Assign a rule to an interface.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 114: Buttons

4.7.3 Overview

This dialog gives you an overview of all the Double NAT rules.

■ Table

Parameter	Meaning
Port	Shows the number of the interface on which the device uses the rule.
Rule Index	Shows the sequential number of the rule.
Rule Name	Shows the name of the rule.
Local Internal IP Address	Shows the local internal IP address of the first subscriber.
Local External IP Address	Shows the local external IP address of the first subscriber into which the device translates the internal local address of the first subscriber.
Remote Internal IP Address	Shows the remote internal IP address of the second subscriber.
Remote External IP Address	Shows the remote external IP address into which the device translates the internal address of the second subscriber.
Trap	Shows whether the device sends an SNMP message (trap) when it uses the rule for data packets. Possible values: ▶ `selected` The device sends a trap. ▶ `not selected` (state on delivery) The device does not send a trap.
Log	Shows whether the device creates log entries when it uses the rule for data packets. Possible values: ▶ `selected` Logging is activated. ▶ `not selected` (state on delivery) Logging is deactivated.
Direction	Shows the data packets to which the rule applies. Possible values: ▶ `ingress` The rule applies to data packets that the interface receives. ▶ egress The rule applies to data packets that the interface sends. ▶ `both` The rule applies to data packets that the interface sends and receives.
Priority	Shows the priority of the rule.

Table 115: "Overview" dialog, table

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 116: Buttons

4.8 DoS

The device provides protection against invalid or fake data traffic that aims to bring down specific services or devices (Denial of Service, DoS). With this menu you can use various filters to restrict the data traffic and protect against Denial of Service attacks.

The menu contains the following dialog:
- Global

4.8.1 Global

With this dialog you can configure the DoS settings for the TCP and ICMP protocols.

- **TCP**
  Network attacks are prepared using what are known as port scans. These attempt to use the network to detect the devices present and the services they provide. This frame allows you to activate or deactivate the detection of these port scans. The device detects the following scan types:
  - Null scan: The device detects TCP packets with no TCP flags set and discards these.
  - Xmas scan: The device detects TCP packets with the TCP flags FIN, URG and PUSH set simultaneously and discards these.
  - SYN/FIN scan: The device detects data packets with the TCP flags SYN and FIN set simultaneously and discards these.
  - Minimal Header scan: The device detects data packets with a TCP header that is too short and discards these.

Parameter	Meaning
Activate Null Scan Filter	Activates or deactivates the Null scan.
Activate Xmas Filter	Activates or deactivates the Xmas scan.
Activate SYN/FIN Filter	Activates or deactivates the SYN/FIN scan.
Activate Minimal Header Filter	Activates or deactivates the Minimal Header scan.

Table 117: "Global" dialog, "TCP" frame

■ IP

This frame allows you to activate or deactivate the Land Attack filter. A Land Attack sends data packets whose source and destination addresses are identical to those of the receiver. When you activate this filter, the device detects data packets with identical source and destination addresses and discards these.

Parameter	Meaning
Activate Land Attack Filter	Activates or deactivates the Land Attack scan.

Table 118: "Global" dialog, "IP" frame

■ ICMP

This dialog provides you with filter options for various ICMP parameters:

- Handling fragmented data packets: When you activate this filter, the device detects fragmented ICMP packets and discards these.
- Allowed size of ICMP packets: Defines the maximum allowed size of ICMP packets in bytes. The device discards data packets that exceed this value.

Parameter	Meaning
Filter Fragmented Packets	Activates or deactivates the filter for fragmented ICMP packets
Allowed Size	Defines the maximum allowed size of ICMP packets.

Table 119: "Global" dialog, "ICMP" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 120: Buttons

4.9 Access Control Lists

In this menu you can enter the settings for the Access Control Lists (ACL).

With the Access Control List, the device filters received data packets at one or more ports. For this, you create rules in the ACL which the device uses to sort incoming packets and frames for an interface or a VLAN. If a rule from the ACL applies to a packet or a frame, the device handles the packet or frame according to the rule you defined (discard, redirect to a specific port, or mirror). You can filter according to the following criteria:

- Source or destination address of a frame (MAC)
- Source or destination address of a data packet (IPv4)
- Type of the transmitting protocol (MAC/IPv4)
- Source or destination port of a data packet (IPv4)
- Service class of a frame (MAC)
- Membership of a specific VLAN (MAC)
- Classification according to DSCP (IPv4)
- Classification according to ToS (IPv4)

The assignment of MAC and IP ACLs to ports and VLANs result in four different types of ACL:

- Port-based MAC ACLs
- VLAN-based MAC ACLs
- Port-based IP ACLs
- VLAN-based IP ACLs

Rules are processed in sequence within an ACL type, namely in the sequence defined by the corresponding rule index. If an ACL is assigned to a port or a VLAN, its priority can be defined within a type by means of a sequence number. The lower the sequence number, the higher the priority. During the processing of the rules, the ACL with the higher priority is always used.

If multiple ACL types contain rules that apply to a data packet, the priority of the ACL type is decisive (not to be confused with the sequence number, which merely defines the sequence within a type). The priority of the ACL types corresponds to the sequence listed above. Therefore, the rules of the port-based IP ACLs have a higher priority than port-based MAC ACLs.

At present you can create up to 128 IP ACLs and 128 MAC ACLs. Each ACL can contain up to 239 rules, but the maximum total number of rules you can create is 956. For each port-based ACL type, a maximum of 239 rules can be active via the assigned ACLs.

For each VLAN-based ACL type, you can assign the ACLs to a maximum of 64 different VLANs at the same time. You can assign a maximum of 176 rules to an ACL type.

The menu contains the following dialogs:

- IPv4 Name
- IPv4 Rule
- MAC Name
- MAC Rule
- Port Assignment
- VLAN Assignment

4.9.1 IPv4 Name

This dialog allows you to create, name, activate and deactivate Access Control Lists for IPv4 addresses.

■ Table

Parameter	Meaning
Index	Shows the sequential number of the rule. The device automatically defines this number.
Name	Here you enter a name for the rule. Possible values: ▶ 1..31 alphanumeric characters
Active	Activates/deactivates the rule. Possible values: ▶ `selected` (state on delivery) The rule is activated. ▶ `not selected` The rule is deactivated.

Table 121: "IPv4 Name" dialog, table

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 122: Buttons

4.9.2 IPv4 Rule

This dialog allows you to define rules for Access Control Lists that apply exclusively to IP data packets.

Table

Parameter	Meaning
Index	Shows the sequential number of the rule.
Name	Displays the name of the rule created in the `Network Security:Access Control Lists:IPv4 Name` dialog.
Match Every IP Packet	Specifies whether the device inspects all IPv4 data packets, regardless of their content.
Source IP Address	The source IP address for which this rule applies. Possible values: ▶ `?.?.?.?` (default setting) The rule applies for every IP address. ▶ Valid IPv4 address The rule applies for the IP address entered exclusively. Use the `?` symbol as a wildcard. For example, enter the value `192.?.?.32`, and the rule applies for every MAC address beginning with `192` and ending with `32`. ▶ Valid IPv4 address/bit mask The bit mask offers the possibility to define every bit of the address range. The rule applies for IP addresses in the address range defined by the bit mask exclusively. For example, enter the value `192.168.1.1/255.255.255.64`, and the rule applies for the IP addresses from `192.168.1.0` to `….127`.
Destination IP Address	The destination IP address for which this rule applies. Possible values: ▶ `?.?.?.?` (default setting) The rule applies for every IP address. ▶ Valid IPv4 address The rule applies for the IP address entered exclusively. Use the `?` symbol as a wildcard. For example, enter the value `192.?.?.32`, and the rule applies for every MAC address beginning with `192` and ending with `32`. ▶ Valid IPv4 address/bit mask The bit mask offers the possibility to define every bit of the address range. The rule applies for IP addresses in the address range defined by the bit mask exclusively. For example, enter the value `192.168.1.1/255.255.255.64`, and the rule applies for the IP addresses from `192.168.1.0` to `….127`.

Table 123:"IPv4 Rule" dialog, table (section 1 of 3)

Parameter	Meaning
Protocol	Shows the transmit protocol for which this rule applies. Possible values: ▶ `0..255` ▶ `inactive` (state on delivery) This criterion is not used for the filtering. ▶ `icmp` ▶ `igmp` ▶ `ip` ▶ `tcp` ▶ `udp`
Source TCP/UDP Port	Defines the source port of the incoming data packets for which this rule applies. Possible values: ▶ `any` The rule applies to data packets of all source ports. ▶ Numeric characters, e.g. `1`
Destination TCP/ UDP Port	Defines the destination port of the incoming data packets for which this rule applies. Possible values: ▶ `any` The rule applies to data packets of all destination ports. ▶ Numeric characters, e.g. `1`
IP DSCP	Defines the DSCP value in the header of a data packet for which this rule applies. Possible values: ▶ `0 (be/cs 0)` ▶ `8 (cs 1)` ▶ `16 (cs 2)` ▶ `24 (cs 3)` ▶ `32 (cs 4)` ▶ `40 (cs 5)` ▶ `48 (cs 6)` ▶ `56 (cs 7)` ▶ `1 - 63` ▶ `-` (state on delivery). This criterion is not used for the filtering.
IP Precedence	Defines the ToS value in the header of a data packet for which this rule applies. Possible values: ▶ `0..7` ▶ `inactive` (state on delivery) This criterion is not used for the filtering.

Table 123:"IPv4 Rule" dialog, table (section 2 of 3)

Parameter	Meaning
TOS/Mask	Defines which bits of the ToS value are to be inspected in the header of the data packet. Possible values: ▶ Numeric characters, e.g. `1` ▶ `inactive` (state on delivery) This criterion is not used for the filtering.
Action	Defines how the device handles incoming IPv4 data packets that this rule applies to. Possible values: ▶ `permit` The device transmits IPv4 data packets to which this rule applies. ▶ `deny` The device discards IPv4 data packets to which this rule applies.
Redirection Port	Defines the device port to which the device forwards received data packets. Only use the "Redirection Port" if you have set the value ‘permit’ in the "Action" column. You have no option of redirecting data packets across VLAN boundaries or to routing interfaces. Possible values: ▶ `inactive` (state on delivery) This rule has no effect on the packet forwarding. ▶ The index number of a device port.
Mirror Port	Defines the device port to which the device forwards copies of the received data packets. Only use the `Mirror Port` if you have set the value "permit" in the "Action" column. You have no option of mirroring data packets across VLAN boundaries or to routing interfaces. Possible values: ▶ `Inactive` This rule has no effect on the packet forwarding. ▶ The index number of a device port.
Active	Activates/deactivates the rule. Possible values: ▶ `selected` (state on delivery) The rule is activated. ▶ `not selected` The rule is deactivated.

Table 123:"IPv4 Rule" dialog, table (section 3 of 3)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 124: Buttons

4.9.3 MAC Name

This dialog allows you to create ACLs for the filtering of MAC frames.

■ Table

Parameter	Meaning
Index	Shows the sequential number of the rule. The device automatically defines this number.
Name	Here you enter a name for the rule. Possible values: ▶ 1..31 alphanumeric characters
Active	Activates/deactivates the rule. Possible values: ▶ `selected` (state on delivery) The rule is activated. ▶ `not selected` The rule is deactivated.

Table 125:"MAC Name" dialog, table

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 126:Buttons

4.9.4 MAC Rule

This dialog allows you to add rules for the filtering of MAC frames to existing ACLs.

■ Table

Parameter	Meaning
Index	Shows the sequential number of the rule.
Name	Displays the name of the rule created in the `Network Security:Access Control Lists:MAC Name` dialog.
Match Every Packet	Specifies whether the device inspects all MAC frames, regardless of their content.
Source MAC Address	Shows the source MAC address for which this rule applies. Possible values: ▶ `??:??:??:??:??:??` (default setting) The rule applies for every MAC address. ▶ Valid MAC address The rule applies for the MAC address entered exclusively. Use the `?` symbol as a wildcard. For example, enter the value `00:11:??:??:??:??`, and the rule applies for every MAC address beginning with `00:11`. ▶ Valid MAC address/bit mask The bit mask offers the possibility to define every bit of the address range. The rule applies for MAC addresses in the address range defined by the bit mask exclusively. For example, enter the value `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`, and the rule applies for the MAC addresses from `00:11:22:33:44:54` to `…:57`.

Table 127: "MAC Rule" dialog, table (section 1 of 3)

Parameter	Meaning
Destination MAC Address	Shows the destination MAC address for which this rule applies. Possible values: ▶ ??:??:??:??:??:?? (default setting) The rule applies for every MAC address. ▶ Valid MAC address The rule applies for the MAC address entered exclusively. Use the ? symbol as a wildcard. For example, enter the value 00:11:??:??:??:??, and the rule applies for every MAC address beginning with 00:11. ▶ Valid MAC address/bit mask The bit mask offers the possibility to define every bit of the address range. The rule applies for MAC addresses in the address range defined by the bit mask exclusively. For example, enter the value 00:11:22:33:44:54/FF:FF:FF:FF:FF:FC, and the rule applies for the MAC addresses from 00:11:22:33:44:54 to …:57.
Ethertype	Shows the Ethertype keyword used in the MAC frame for which this rule applies. Possible values: ▶ custom Uses the value specified in the "Ethertype Custom Value" field. ▶ appletalk ▶ arp ▶ ibmsna ▶ ipv4 ▶ ipv6 ▶ ipxold ▶ mplsmcast ▶ mplsucast ▶ netbios ▶ novell ▶ pppoedisc ▶ ppoesess ▶ ipx-new ▶ profinet ▶ powerlink ▶ ethercat ▶ rarp
Ethertype Custom Value	Specifies the Ethertype value to be used for filtering (e.g. 0x0800 for Ethernet frames with IP data). This value can also be used to filter LLC frames based on their length field. If you use values smaller than 1535 for this, the system automatically filters based on LLC frames of the specified size. Filtering based on the length field is only available to you for port-based ACLs. With Ethertype “custom(1)” and Ethertype value 0, filtering based on Ethertype is inactive.

Table 127:"MAC Rule" dialog, table (section 2 of 3)

Parameter	Meaning
VLAN ID	The VLAN ID of incoming data packets for which this rule applies. Possible values: ▶ 1.. 4042
COS	Defines the Class of Service used in a VLAN tag for which this rules applies. Please note that for frames without a VLAN tag, the port priority is automatically used for filtering instead of the CoS value.
Action	Defines how the device handles incoming data packets that this rule applies to. Possible values: ▶ `permit` The device transmits data packets to which this rule applies. ▶ `deny` The device discards data packets to which this rule applies.
Redirection Port	Defines the routing interface to which the device forwards received data packets. Only use the "Redirection Port" if you have set the value "permit" in the `Action` column. You have no option of redirecting data packets across VLAN boundaries or to routing interfaces. Possible values: ▶ `Inactive` This rule has no effect on the packet forwarding. ▶ <Port number> The device forwards received data packets to the defined interface.
Mirror Port	Defines the routing interface to which the device forwards copies of the received data packets. Only use the `Mirror Port` if you have set the value "permit" in the "Action" column. You have no option of mirroring data packets across VLAN boundaries or to routing interfaces. Possible values: ▶ `Inactive` This rule has no effect on the packet forwarding. ▶ <Port number> The device forwards copies of the received data packets to the specified port.
Active	Activates/deactivates the rule. Possible values: ▶ `selected` (state on delivery) The rule is activated. ▶ `not selected` The rule is deactivated.

Table 127:"MAC Rule" dialog, table (section 3 of 3)

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 128: Buttons

4.9.5 Port Assignment

With this dialog you can assign the ACLs to specific ports.

■ Table

Parameter	Meaning
Name	Shows the name of the ACL rule.
Type	Shows whether the rule is MAC- or IPv4-based.
Port	Defines the port for which this rule applies.
Direction	Shows the data packets to which the rule applies. You define the value by clicking on the "Assign" button. Possible values: ▶ `inbound` The rule applies to data packets that the interface receives.
Sequence	Defines the priority of the rule when it is used on a routing interface, when the routing interface has multiple rules.
Active	Activates/deactivates the rule. Possible values: ▶ `selected` (state on delivery) The rule is activated. ▶ `not selected` The rule is deactivated.

Table 129: "Port Assignment" dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Assign	Assign a rule to an interface.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 130: Buttons

4.9.6 VLAN Assignment

This dialog allows you to assign the ACLS to individual VLANs.

■ Table

Parameter	Meaning
Name	Shows the name of the ACL rule.
Type	Shows whether the rule is MAC- or IPv4-based.
VLAN	Defines the VLAN for which this rule applies.
Direction	Shows the data packets to which the rule applies. You define the value by clicking on the "Assign" button. Possible values: ▶ `inbound` The rule applies to data packets that the interface receives.
Sequence	Defines the priority of the rule when it is used on a routing interface, when the routing interface has multiple rules.
Active	Activates/deactivates the rule. Possible values: ▶ `selected` (state on delivery) The rule is activated. ▶ `not selected` The rule is deactivated.

Table 131:"VLAN Assignment" dialog

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Assign	Assign a rule to an interface.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 132:Buttons

5 Switching

With this menu you can configure the settings for the switching.

The menu contains the following dialogs:
- Switching Global
- Filter for MAC addresses
- VLAN

5.1 Switching Global

This dialog allows you to configure basic settings for the switching.

If very many large data packets are received at a device port at the same time, this can cause the port memory to overflow. The device then discards the surplus data packets.

Example: The device receives data at a Gigabit port and forwards it to a port with a lower bandwidth.

The flow control mechanism described in standard IEEE 802.3 ensures that no data packets are lost due to a port memory overflowing. Shortly before a port memory is completely full, the device signals to the connected devices that it is not accepting any more data packets from them.

- In full-duplex mode, the device sends a pause data packet.
- In half-duplex mode, the device simulates a collision.

After this, the connected devices do not send any more data packets, neither to the signaling device nor to the other devices. On uplink ports, this can possibly cause undesired sending breaks in the higher-level network segment (“wandering backpressure”).

Configuration

Parameters	Meaning
MAC Address	Displays the MAC address of the device.
Aging Time (s)	Defines the aging time in seconds. Possible values: ▶ 10..500000 (default setting: 30) The device monitors the age of the learned Unicast MAC addresses. Address entries that exceed a particular age (aging time) are deleted by the device from its address table (FBD, Forwarding Database). You will find the address table in the Switching:Filter for MAC addresses dialog. In connection with the router redundancy, select a time ≥ 30 s.
Activate Flow Control	Activates/deactivates the flow control globally in the device. Possible values: ▶ Not selected (default setting) ▶ Selected For this, you also activate the "Flow Control" function for the device ports in the Basic Settings:Port Configuration dialog.

Table 133: "Switching Global" dialog, "Configuration" frame

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 134: Buttons

5.2 Filter for MAC addresses

The "Filter for MAC Addresses" table allows you to display and edit address filters for the forwarding table. Address filters define the way the data packets are transmitted in the device based on the destination MAC address.

Each row in the table represents one filter. The device automatically sets up the filters. The device allows you to set up additional filters manually.

The device transmits the data packets as follows:

- If the table contains an entry for the destination address of a data packet, the device transmits the data packet from the receiving port to the port specified in the table entry.
- If there is no table entry for the destination address, the device transmits the data packet from the receiving port to all the other ports.

■ Table

Parameters	Meaning
Address	Shows the destination MAC address to which the table entry applies.
Status	Shows how the device has set up the address filter. Possible values: ▶ `learned` Address filter set up automatically by the device based on received data packets. ▶ `permanent` Address filter set up manually. The address filter stays set up permanently. ▶ `mgmt` MAC address of the device. The address filter is protected against changes. ▶ `invalid` Deletes a manually set up address filter.
VLAN ID	Shows the ID of the VLAN to which the table entry applies. Possible values: ▶ `1..4042` The device learns the MAC addresses for every VLAN separately (independent VLAN learning).
Ports	Shows how the corresponding device port transmits data packets for the adjacent destination address. Possible values: ▶ `-` The port does not transmit any data packets to the destination address. ▶ `learned` The port transmits data packets to the destination address. The device sets up the filter automatically based on received data packets. ▶ `unicast static` The port transmits data packets to the destination address. A user created the filter. ▶ `multicast static` The port transmits data packets to the destination address. A user created the filter.

Table 135: "Filters for MAC Addresses" dialog, table

To remove the learned MAC addresses from the forwarding table, click `Reset MAC Address Table` in the "Basic Settings:Restart" dialog.

Create

To set up a filter manually, click the "Create" button.

Parameters	Meaning
VLAN ID	Defines the ID of the VLAN to which the table entry applies. Possible values: ▶ All VLAN IDs that are set up
Address	Defines the destination MAC address to which the table entry applies. Possible values: ▶ Valid MAC address Enter the value in one of the following formats: – without a separator, e.g. `001122334455` – separated by spaces, e.g. `00 11 22 33 44 55` – separated by colons, e.g. `00:11:22:33:44:55` – separated by hyphens, e.g. `00-11-22-33-44-55` – separated by points, e.g. `00.11.22.33.44.55` – separated by points every 4th character, e.g. `0011.2233.4455`
Possible Ports	Defines the device ports to which the device transmits data packets with the destination MAC address: □ Select one port if the destination MAC address is a Unicast address. □ Select one or more ports if the destination MAC address is a Multicast address. □ Select no port to set up a discard filter. The device discards data packets with the destination MAC address specified in the table entry.

Table 136:"Create" dialog

Edit Entry

To manually adapt the settings for a table entry, click the "Edit Entry" button.

Parameters	Meaning
Possible Ports	This column contains the ports available in the device.
Dedicated Ports	This column contains the device ports that are assigned to the table entry. □ Select one port if the destination MAC address is a Unicast address. □ Select one or more ports if the destination MAC address is a Multicast address. □ Select no port to set up a discard filter. The device discards data packets with the destination MAC address specified in the table entry.

Table 137:"Filters for MAC Addresses" dialog, "Edit Entry" frame

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Create	Adds a new table entry.
Edit Entry	Shows the "Edit Entry" frame. See “Edit Entry” on page 170.
Help	Opens the online help.
>	Moves the selected entry to the right column.
>>	Moves all entries to the right column.
<	Moves the selected entry to the left column.
<<	Moves all entries to the left column.

Table 138: Buttons

5.3 VLAN

With VLAN (Virtual Local Area Network) you distribute the data traffic in the physical network to logical subnetworks. This provides you with the following advantages:

- High flexibility
  - With VLAN you distribute the data traffic to logical networks in the existing infrastructure. Without VLAN, it would be necessary to have additional devices and complicated cabling.
  - With VLAN you define network segments independently of the location of the individual terminal devices.
- Improved throughput
  - In VLANs data packets can be transferred by priority.
    If the priority is high, the device transfers the data traffic of a VLAN preferentially, e.g. for time-critical applications such as VoIP phone calls.
  - The network load is considerably reduced if data packets and Broadcasts are distributed in small network segments instead of in the entire network.
- Increased security
  The distribution of the data traffic among individual logical networks makes unwanted accessing more difficult and strengthens the system against attacks such as MAC Flooding or MAC Spoofing.

The device supports packet-based “tagged” VLANs according to the IEEE 802.1Q standard. The VLAN tagging in the data packet indicates the VLAN to which the data packet belongs.

The device transmits the tagged data packets of a VLAN exclusively via ports that are assigned to the same VLAN. This reduces the network load.

Depending on the settings, we differentiate between the following VLANs:

- Static VLANs
  VLANs set up manually by the user.
- Dynamic VLANs
  VLANs set up automatically by the following mechanisms:
  - Routing (routing is activated on the port)
  - Redundancy mechanisms

The device learns the MAC addresses for every VLAN separately (independent VLAN learning).

The menu contains the following dialogs:

- Global
- Current
- Static
- Port

5.3.1 Global

This dialog allows you to view general VLAN parameters for the device.

Configuration

Parameters	Meaning
Max. VLAN ID	Biggest ID that you can assign to a VLAN. See the `Switching:VLAN:Static` dialog.
Max. Number of VLANs	Maximum number of VLANs that you can set up in the device. See the `Switching:VLAN:Static` dialog.
Number of VLANs	Number of VLANs currently set up in the device. See the `Switching:VLAN:Static` dialog. The VLAN with ID 1 is always set up in the device.

Table 139:"Global" dialog, "Configuration" frame

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 140:Buttons

5.3.2 Current

This dialog allows you to view the static and dynamic VLANs that are set up. The table shows the ports to which the device distributes the data packets for the corresponding VLAN, and how the port handles the tagging of the data packets. You can make changes to the entries in the `Switching:VLAN:Static` dialog.

■ Table

Parameters	Meaning
VLAN ID	ID of the VLAN.
Status	Shows how the VLAN is set up. Possible values: ▶ `other` Only for VLAN 1. ▶ `permanent` Manually set up VLAN. If the device is reset, the configuration of this VLAN remains in the device.
Creation Time	Shows the time stamp for the operating time (system uptime). The VLAN has been set up in the device since this time. Possible values: ▶ day(s), hh:mm:ss
Port	Shows on which ports the device transmits the data packets for the corresponding VLANs, and how it handles the VLAN tagging. Possible values: ▶ `-` The port does not transmit any data packets for the VLAN. The port is not a member of the VLAN. ▶ `T` The port transmits data packets with a VLAN tag (tagged). ▶ `U` The port transmits data packets without a VLAN tag (untagged).

Table 141: "Current" dialog, table

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 142: Buttons

5.3.3 Static

This dialog allows you to create and manage VLANs. In the table you assign the VLANs that are set up to the device ports. In the process you define whether a port transmits data packets in the corresponding VLAN, and how the port handles the VLAN tagging.

■ Table

Parameters	Meaning
VLAN ID	ID of the VLAN. The device supports up to 64 VLANs set up simultaneously. Possible values: ▶ `1..4042`
Name	Name of the VLAN. The device automatically specifies the name. You can change the name at any time. Possible values: ▶ 1..32 alphanumeric characters (state on delivery: `default` for VLAN 1, otherwise `VLANxxxx`)
Port	Defines on which ports the device transmits the data packets for the corresponding VLANs, and how it handles the VLAN tagging. Possible values: ▶ `-` (state on delivery) The port does not transmit any data packets for the VLAN. The port is not a member of the VLAN. ▶ `T` The port transmits data packets with a VLAN tag (tagged). You use this setting for an uplink connection, for example. ▶ `U` (state on delivery for VLAN 1) The port transmits data packets without a VLAN tag (untagged). Use this setting if the connected terminal device does not evaluate any VLAN tags. ▶ `F` The port does not transmit any data packets, neither from static nor dynamic VLANs (forbidden). Use this setting if the connected terminal device does not evaluate any VLAN tags.

Table 143: "Static" dialog, table

The device automatically creates a VLAN for every port on which routing is activated. When you deactivate the routing on a port, the device removes the related VLAN again.

Note: When configuring the VLAN, ensure that the management station still has access to the device after the VLAN configuration is saved. Connect the management station to a port that is a member of the VLAN that is selected as the management VLAN. In the state on delivery, the device transmits the management data in VLAN 1.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 144: Buttons

5.3.4 Port

This dialog allows you to assign a VLAN to the device ports and thus define the port VLAN ID.
Additionally, you also define for each device port how the device transmits data packets if one of the following situations occurs:

- The port receives data packets without a VLAN tagging.
- The port receives data packets with VLAN priority information (VLAN ID 0, priority tagged).
- The VLAN tagging of the data packet differs from the VLAN ID of the port.

■ Table

Parameters	Meaning
Port	Device port to which the table entry relates.
Port VLAN ID	The port assigns to this VLAN data packets that have no VLAN tagging or are tagged with VLAN ID 0. This setting is effective if you have selected the value "admitAll" in the Acceptable Frame Types column. Possible values: ▶ All VLAN IDs that are set up (default setting: 1)
Acceptable Frame Types	Defines whether the port transmits or discards received data packets without a VLAN tagging or data packets with VLAN priority information (VLAN ID 0, priority tagged): ▶ admitAll (default setting) The port transmits data packets with or without a VLAN tag. ▶ admitOnlyVlanTagged The port only transmits data packets tagged with a VLAN ID ≥ 1.
Ingress Filtering	Defines whether the port transmits or discards received data packets with a VLAN tagging. ▶ selected (default setting) The device compares the VLAN tagging in the data packet with the VLANs to which the device sends on this port according to the Switching:VLAN:Static dialog. If the VLAN tagging in the data packet matches one of these VLANs, the port forwards the data packet to ports in this VLAN. Otherwise the port discards the data packet. ▶ not selected The port forwards data packets received with a VLAN tagging to other ports without comparing the VLAN IDs. Thus the port also transmits data packets with a VLAN tagging even though it is not a member of this VLAN.

Table 145: Dialog "Port"

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 146: Buttons

6 Routing

With this menu you can configure the settings for routing.

For security reasons, the following functions are permanently disabled in the device:

- Source Routing
  With source routing, the data packet contains the routing information and overwrites the settings in the router with it.
- ICMP Redirects
  The routing table can be manipulated by ICMP redirect data packets. The device generally ignores received ICMP redirect data packets. The settings in the `Routing:Interfaces:Configuration` dialog, "ICMP Redirects" field has no effect on this.

In accordance with RFC 2644, the device does not exchange any broadcast data packets from external networks in a local network. This behavior supports you in protecting the devices in the local network against overloading, for example due to so-called smurf attacks.

The menu contains the following dialogs:

- Global
- Interfaces
- Routing Table

6.1 Global

This dialog gives you the option of enabling the routing function in the device. In addition the dialog displays the preset TTL (time to live) for data packets that the management of the device sends.

■ Operation

Parameters	Meaning
Operation	When the function is switched on, routing is activated globally in the device. Possible values: ▶ `Off` (default setting) Function is switched off. ▶ `On` Function switched on.

Table 147:"Routing Global"dialog, "Operation" frame

■ Information

Parameters	Meaning
Default TTL	In addition the dialog displays the default TTL (time to live) for data packets that the management of the device sends. Possible values: ▶ `64` (default setting) The forwarding router reduces the value in the data packet by `1` on the transmission path. If a router receives a data packet with the TTL value `1`, it discards the data packet. The router also reports that it has discarded the data packet to the source IP address.

Table 148:"Routing Global"dialog, "Operation" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 149: Buttons

6.2 Interfaces

With this menu you can configure the settings for the individual router interfaces.

The menu contains the following dialogs:
- Configuration
- Secondary Interface addresses

6.2.1 Configuration

This dialog gives you the following options:
- Assigning an IP address and network mask to a particular router interface.
- Enabling/disabling the routing function for a particular router interface.
- Enabling/disabling the proxy ARP function for a particular router interface.
- Entering an MTU value for a particular routing interface.
- Setting whether a certain router interface sends an unreachable message if a network or destination computer cannot be reached.
- Setting whether ICMP redirects are sent on a router interface if the destination can be reached directly or via another router.

■ Table

Parameters	Meaning
Port	Device port to which the table entry relates.
Type	Displays whether the router interface is a device port or a virtual port. Possible values ▶ `Ethernet` Device port ▶ `VLAN` Virtual, VLAN-based port
VLAN ID	Displays the ID of the VLAN for virtual ports.
IP Address	Defines the IP address for the router interface. Possible values: ▶ Valid IPv4 address (default setting: `0.0.0.0`)
Netmask	Defines the network mask for the router interface. Possible values: ▶ Valid IPv4 network mask (default setting: `0.0.0.0`)
Routing	Enables/disables the routing function on the router interface. Possible values: ▶ `selected` Routing function enabled. – With port-based routing, the device transforms the device port into a routing interface. Enabling the routing function removes the port from the VLANs in which it was previously a member. Disabling the routing function does not reestablish the assignment; the port is not a member of any VLAN. – With VLAN-based routing, the device activates forwarding of data packets. ▶ `not selected` (default setting) Routing function disabled. With VLAN-based routing, the device can be reached via its IP parameters, if the IP address and network mask have been configured.
Proxy ARP	Enables/disables the proxy ARP function for the router interface. This function gives you the option of integrating remote devices. Possible values: ▶ `selected` Proxy ARP function enabled. ▶ `not selected` (default setting) Proxy ARP function inactive.
MTU Value	Specifies the maximum permissible network packet size.

Table 150: "Configuration" dialog, table

Parameters	Meaning
ICMP Unreachables	Shows whether the device sends ICMP unreachable messages for this router interface. Possible values: ▶ `enable` The device sends ICMP unreachable messages. ▶ `disable` The device does not send ICMP unreachable messages.
ICMP Redirects	Shows whether the device sends ICMP redirect messages for this router interface. Possible values: ▶ `enable` The device sends ICMP redirect messages. ▶ `disable` The device does not send ICMP redirect messages.

Table 150: "Configuration" dialog, table (Cont.)

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Remove	Removes the selected table entry.
Wizard	Opens the "Wizard".
Help	Opens the online help.

Table 151: Buttons

■ Wizard – page “Create or select VLAN”

Parameter	Meaning
VLAN ID	Displays the ID of the VLAN. Possible values: ▶ `1..4042`
VLAN Name	Displays the name of the VLAN.

Table 152: Wizard – page "Create or select VLAN"

■ Wizard – page “Setup VLAN”

Parameter	Meaning
VLAN ID	You specify the ID of the VLAN here.
VLAN Name	You specify the name of the VLAN here. Possible values: ▶ Alphanumeric characters
Port	Port to which this entry applies.
Member	You enable or disable the membership of the router interface to a VLAN here.
Untagged	You enable or disable whether the router interface is available for one or more VLANs here. If you activate the option, the router interface is exclusively available for one VLAN.
Port VLAN ID	Specifies which VLAN ID receives packets without their own VLAN ID.

Table 153: Wizard – page "Setup VLAN"

■ Wizard – page “Setup virtual routerport”

Parameter	Meaning
Address	Identifies the IP address of the virtual routerport.
Netmask	Displays the network mask of the respective IP address.

Table 154: Wizard – page "Setup virtual routerport"

Button	Meaning
Add	Adds the values entered in the fields “Address” and “Netmask” in the list for other addresses. The device uses the IP addresses from this list for multinetting.
Remove	Removes the selected entry from the “Secondary Interface addresses” list.

Table 155: “Configuring VLAN router interfaces“, page “Setup virtual routerport”

6.2.2 Secondary Interface addresses

This dialog displays an overview of IP addresses that are available to a router interface during multinetting. Multinetting is the option of assigning several IP addresses to a router interface. Use this function if you connect a physical medium, which has several existing subnetworks, to the router interface.
In this dialog you have the following options:

- Adding an IP address for multinetting
- Removing an IP address for multinetting

Note: You have the option to configure a secondary IP addresses for each router interface up to a total of up to 64 secondary IP addresses per device.

Table

Parameter	Meaning
Port	Device port to which the table entry relates.
IP Address	Displays the IP address for this entry.
Netmask	Displays the network mask for this entry.

Table 156: "Secondary Interface addresses" dialog

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Add IP Address	Opens the "Create" dialog. This dialog gives you the option of adding a further IP address to a router interface. Enter the desired value in the "IP Address" and "Netmask" fields. Confirm the entry by clicking on "OK".
Delete IP Address	This dialog gives you the option of deleting an IP address for a router interface. Select an IP address in the list and then click "Delete IP Address".
Help	Opens the online help.

Table 157: Buttons

6.3 Routing Table

This menu gives you the option of viewing the dynamic and static routing table. In addition, you can configure the static routing table.

The menu contains the following dialogs:

- Current
- Static

6.3.1 Current

This dialog displays all routes that are currently configured on the device. The device uses these routes for the exchange decision.

■ Table

Parameter	Meaning
Port	The port that belongs to this entry.
Network address	IP address of the destination network
Netmask	Network mask for the IP address of the destination network
Next Hop IP Address	IP address of the next router on the path to the destination network.
Type	Displays whether the destination can be reached via the router interface. Possible values: ▶ `local` The destination can be reached directly via this router interface. ▶ `remote` The destination can be reached via other router interfaces.
Protocol	Displays which route this entry has generated. Possible values: ▶ `local` The local router interface generated this entry. ▶ `netmgmt` A static route generated this entry. ▶ `ospf` A route via the open shortest path first protocol generated this entry. ▶ `rip` A route via the routing information protocol generated this entry.
Metric 1	Displays the primary metric of this route.
Metric 2 Metric 3 Metric 4 Metric 5	Displays the other metrics of this route.
Last Update [s]	Shows the time in seconds that has elapsed since the last update of the route.

Table 158: "Current routing table" dialog, table

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 159: Buttons

6.3.2 Static

This dialog allows you to configure static routes.

Table

Parameter	Meaning
Port	The port that belongs to this entry.
Network address	IP address of the destination network
Netmask	Network mask for the IP address of the destination network
Next Hop IP Address	IP address of the next router on the path to the destination network.
Type	Displays whether the destination can be reached via the router interface. Possible values: ▶ `local` The destination can be reached directly via this router interface. ▶ `remote` The destination can be reached via other router interfaces.
Metric 1	Displays the primary metric of this route.
Metric 2 Metric 3 Metric 4 Metric 5	Displays the other metrics of this route.
Active	Displays whether the route is active.

Table 160: "Static routing table" dialog, table

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 161: Buttons

7 QoS/Priority

Communication networks transmit a number of applications at the same time that have different requirements as regards availability, bandwidth and latency periods.

QoS (Quality of Service) is a procedure defined in IEEE 802.1D. It is used to distribute resources in the network. You therefore have the possibility of providing minimum bandwidth for important applications. Prerequisite for this is that the end devices and the devices in the network support prioritized data transmission. Data packets with high priority are given preference when transmitted by devices in the network. You transfer data packets with lower priority when there are no data packets with a higher priority to be transmitted.

The device provides the following setting options:

- You specify how the device evaluates QoS/prioritization information for inbound data packets.
- For outbound packets, you specify which QoS/prioritization information the device writes in the data packet (e.g. priority for management packets, port priority).

Note: Switch off flow control if you use the functions in this menu. The flow control is switched off if "Activate Flow Control" is unselected in the `Switching:Global` dialog, "Configuration" frame .

The menu contains the following dialogs:

- Global
- Port Configuration
- 802.1D/p Mapping
- Queue Management

7.1 Global

The device allows you to maintain access to the management functions, even in situations with heavy utilization. In this dialog you define the required QoS/priority settings.

■ Configuration

Parameters	Meaning
VLAN Priority for Management packets	Defines the VLAN priority for management data packets to be sent. The device sends the management data packets with the priority specified here. Possible values: ▶ `0..7` (default setting: `0`) In the `QoS/Priority:802.1D/p Mapping` dialog you assign the VLAN priority to the traffic classes and thus the data packets to a priority queue of the port.
IP-DSCP Value for Management packets	Defines the DSCP value for data packets that the management of the device sends. Possible values: ▶ `0..63` (default setting: `0(be/cs0)`) Some values in the list also have a DSCP keyword, e.g. `be/cs0`, `af11` and `ef`. These values are compatible with the IP precedence model.
Number of Queues per Port	Shows the number of priority queues per device port. Every priority queue is assigned traffic classes (traffic class based on IEEE 802.1D). The device supports 8 priority queues.

Table 162:“Global” dialog, "Configuration" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 163: Buttons

7.2 Port Configuration

In this dialog you define the QoS/priority settings for each device port for received data packets.

Table

Parameters	Meaning
Port	Device port to which the table entry relates.
Port Priority	Defines the port priority. The device exchanges the data packets received on the port according to the assigned traffic class. Possible values: ▶ `0..7` (default setting: `0`) Prerequisite: The data packets do not contain a VLAN tag or priority tag. The `QoS/Priority:802.1D/p Mapping` dialog shows which traffic class has been assigned to the respective VLAN priority. The device assigns the data packets to a traffic class depending on their VLAN priority and thereby sorts them in the priority queue.

Table 164: "Port Configuration" dialog, table

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 165: Buttons

7.3 802.1D/p Mapping

The device allows you send data packets with a VLAN tagging according to the QoS/priority information contained in the data packet with a higher or lower priority.

In this dialog you assign the VLAN priority to the traffic classes. The traffic classes are assigned to the priority queues of the device ports.

■ Table

To change the settings click the desired row of the "Traffic Class" column and modify the value.

Parameters	Meaning
VLAN Priority	VLAN priority of received data packets.
Traffic Class	Defines the traffic class. Possible values: ▶ `0..7` The traffic classes are assigned to the priority queues of the device ports: ▶ Traffic class `7` … queue with the highest priority ▶ Traffic class `0` … queue with the lowest priority

Table 166: "802.1D/p Mapping" dialog, table

VLAN Priority	Traffic class	Content description according to IEEE 802.1D
0	2	Best Effort Normal data without prioritizing.
1	0	Background Non-time critical data and background services.
2	1	Standard Normal data.
3	3	Excellent Effort Important data.
4	4	Controlled load Time-critical data with a high priority.
5	5	Video Video transmission with delays and jitter < 100 ms.
6	6	Voice Voice transmission with delays and jitter < 10 ms.
7	7	Network Control Data for network management and redundancy mechanisms.

Table 167: Default assignment of the VLAN priority to the traffic classes

Note: Network management protocols and redundancy mechanisms use the highest traffic class. Therefore, select another traffic class for application data.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 168: Buttons

7.4 Queue Management

With this dialog you can activate/deactivate the "Strict Priority" function for the traffic classes. When the "Strict Priority" function is switched off, the device controls the processing of the priority queue with Weighted Fair Queuing.

■ Table

Parameters	Meaning
Traffic Class	Traffic class assigned to a priority queue of the ports.
Strict Priority	Displays that the device is processing the priority queue of the ports with "Strict Priority" for this traffic class. The device port only sends data packets that are in the priority queue with the highest priority. If this priority queue is empty, the device port sends data packets that are in the priority queue with the next lower priority. The device port only sends data packets with a lower traffic class when the priority queues with a higher priority are empty. In unfavorable situations, the device port never sends these data packets.

Table 169:“Queue Management” dialog, table

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 170:Buttons

8 Diagnostics

The dialogs in this menu show information on statuses and events that the device has logged. In service cases, this information helps our support to diagnose the situation.

The menu contains the following dialogs:

- Report
- Ports
- Configuration Check
- ARP
- Device Status
- Signal Contact
- Alarms (Traps)
- Selftest

8.1 Report

The device allows you to log user actions and device-specific events. In this menu you configure the logging settings for the device. You also have the option to view the reports.

The menu contains the following dialogs:

- Global
- Syslog
- Persistent Logging
- System Log
- System Information
- Audit Trail

8.1.1 Global

The device allows you to log specific events using the following outputs:

- on the console
- on one or more syslog servers
- on a CLI connection set up using SSH

You define the required settings in this dialog. By assigning the severity you define which events the device logs.

The buttons in the dialog allow you to save a ZIP archive with system information and the Java Applet of the graphic user interface (GUI) on your PC.

Console Logging

Parameters	Meaning
Operation	When the function is switched on, the device logs the events on the console. Possible values: ▶ `On` ▶ `Off` (default setting)
Severity	Defines the minimum severity for the events. The device logs all events with this severity and with more urgent severities. The device outputs the messages on the V.24 interface. Possible values: ▶ `emergency` ▶ `alert` ▶ `critical` ▶ `error` ▶ `warning` (default setting) ▶ `notice` ▶ `informational` ▶ `debug`

Table 171: "Global" dialog, "Console Logging" frame

■ Buffered Logging

The device buffers logged events in 2 separate storage areas so that the log entries for urgent events are kept.

This dialog allows you to define the minimum severity for events that the device buffers in the storage area with a higher priority.

Parameters	Meaning
Severity	Defines the minimum severity for the events. The device buffers log entries for events with this severity and with more urgent severities in the storage area with a higher priority. Possible values: ▶ `emergency` ▶ `alert` ▶ `critical` ▶ `error` ▶ `warning` (default setting) ▶ `notice` ▶ `informational` ▶ `debug`

Table 172: "Global" dialog, "Buffered Logging" frame

■ CLI Logging

Parameters	Meaning
Operation	When the function is switched on, the device logs all commands received through Command Line Interface (CLI). Possible values: ▶ `On` ▶ `Off` (default setting)

Table 173: "Global" dialog, "CLI Logging" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Download Support Information	Opens the "Save" dialog. This dialog allows you to save a ZIP archive on your PC that contains system information about the device. The device generates the file name of the ZIP archive automatically based on the format <IP address>_<device name>.zip. You will find an explanation of the files contained in the ZIP archive in the following section.
Download JAR File	Opens the "Save" dialog. The dialog allows you to save the Java Applet of the graphic user interface (GUI) on your PC as a JAR file. When you start the JAVA Applet, you have the option of administering the device, even if its HTTP server is switched off for security reasons. The device generates the file name of the Java Applet automatically based on the format <product>-<software version)>-<build no.>.jar.
Help	Opens the online help.

Table 174: Buttons

Support Information: Files contained in ZIP archive

System information	File name	Format	Comments
Output of CLI commands: ▶ show port all ▶ show system info ▶ show mac-addr-table ▶ show mac-filter-table igmp-snooping	CLICommands.txt	Text	Prerequisite: The Telnet server of the device is switched on.
Default device configuration	defaultconfig.xml	XML	Device configuration with the plant settings.
Device configuration	runningconfig.xml	XML	Device configuration that the device uses in the current operation.
Support Information	supportinfo.html	Text	Device internal service information.
System information	systeminfo.html	HTML	—
Log file	systemlog.html	HTML	—

Table 175: Support Information: Files contained in the ZIP archive

Meaning of the severities for events

Severity	Meaning
`emergency`	Device not ready for operation
`alert`	Immediate user intervention required
`critical`	Critical status
`error`	Error status
`warning`	Warning
`notice`	Significant, normal status
`informational`	Informal message
`debug`	Debug message

Table 176: Meaning of the severities for events

8.1.2 Syslog

The device enables you to send specific logged events to one or more syslog servers. In this dialog you define the settings for this.

The dialog manages a list of up to 8 syslog server entries. Depending on the severity of the event, the device sends the log entry to different syslog servers.

■ Operation

Parameters	Meaning
Operation	When the function is switched on, the device sends the events specified in the table to the specified syslog servers. Possible values: ▶ `On` ▶ `Off` (default setting)

Table 177: "Syslog" dialog, "Operation" frame

■ Table

Parameters	Meaning
Index	Shows a sequential number to which the table entry relates. The device automatically defines this number. When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap. Possible values: ▶ `1..8`
IP Address	Specifies the IP address of the syslog server. Possible values: ▶ Valid IPv4 address (default setting: `0.0.0.0`)
Port	Defines the UDP Port on which the syslog server expects the log entries. Possible values: ▶ `1..65535` (default setting `514`)
Minimum Severity	Defines the minimum severity of the events. The device sends a log entry for events with this severity and with more urgent severities to the syslog server. Possible values: ▶ `emergency` ▶ `alert` ▶ `critical` ▶ `error` ▶ `warning` (default setting) ▶ `notice` ▶ `informational` ▶ `debug`
Type	Defines the type of the log entry transmitted by the device. Possible values: ▶ `systemlog` (default setting)
Active	Activates/deactivates the transmission of events to the syslog server: ▶ `selected` The device sends events to the syslog server. ▶ `not selected` (default setting) The transmission of events to the syslog server is deactivated.

Table 178:"Syslog" dialog, table

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 179: Buttons

8.1.3 Persistent Logging

The device allows you to save all log entries permanently in a file on the external memory. Therefore, even after the device is restarted you have access to the log entries.

With this dialog you can limit the size of the log file and define the minimum severity for the events to be saved. If the log file attains the specified size, the device archives this file and saves the following log entries in a newly created file.

In the table the device shows you the log files held on the external memory. As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files. This ensures that there is always enough memory space on the external memory.

■ Operation

Parameters	Meaning
Operation	When the function is switched on, the device saves the log entries in a file on the external memory. Possible values: ▶ `On` (default setting) ▶ `Off` Only activate this function when the external memory is available on the device.

Table 180: "Persistent Logging" dialog, "Operation" frame

Configuration

Parameters	Meaning
Max File Size	Defines the maximum size of the log file in KBytes. If the log file attains the specified size, the device archives this file and saves the following log entries in a newly created file. Possible values: ▶ `0..4096` (default setting `1024`) The value `0` deactivates saving of log entries in the log file.
Max Files	Defines the number of log files that the device keeps on the external memory. As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files. Possible values: ▶ `0..25` (default setting `4`) The value `0` deactivates saving of log entries in the log file.
Severity	Defines the minimum severity of the events. The device saves the log entry for events with this severity and with more urgent severities in the log file on the external memory. Possible values: ▶ `emergency` ▶ `alert` ▶ `critical` ▶ `error` ▶ `warning` (default setting) ▶ `notice` ▶ `informational` ▶ `debug`

Table 181:"Persistent Logging" dialog, "Configuration" frame

Table

Parameters	Meaning
Index	Shows a sequential number to which the table entry relates. Possible values: ▶ 1..25 The device automatically defines this number.
File Name	Shows the file name of the log file on the external memory. Possible values: ▶ messages ▶ messages.X
File Size	Shows the size of the log file on the external memory in bytes.

Table 182: "Persistent Logging" dialog, table

To delete the log files, click "Delete Persistent Log File" in the Basic Settings:Restart dialog.
See “Restart” on page 44.

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 183: Buttons

8.1.4 System Log

The device logs important device-internal events in a log file (system log).

This dialog displays the log file (system log). The dialog allows you to search the log file for search terms and save them in HTML format on your PC.

The log file is kept until a cold start is performed on the device. After the cold start the device creates the file again.
To delete the logged events from the log file, click `Delete Log File` in the "Basic Settings:Restart" dialog.

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Search	Opens the "Search" dialog. The dialog allows you to search the log file for search terms or regular expressions.
Save	Opens the "Save" dialog. The dialog allows you to save the log file in HTML format on your PC.
Help	Opens the online help.

Table 184:Buttons

8.1.5 System Information

This dialog displays the current operating condition of individual components in the device. The displayed values are a snapshot; they represent the operating condition at the time the dialog was loaded to the page.

The dialog allows you to search the page for search terms and save them in HTML format on your PC.

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Search	Opens the "Search" dialog. The dialog allows you to search the log file for search terms or regular expressions.
Save	Opens the "Save" dialog. The dialog allows you to save the log file in HTML format on your PC.
Help	Opens the online help.

Table 185: Buttons

8.1.6 Audit Trail

The device logs system events and writing user actions on the device. This gives you the option of following WHO changes WHAT on the device WHEN. The logged entries are write-protected and remain saved in the device after a cold reset.

This dialog displays the log file (audit trail). The dialog allows you to search the log file for search terms and save them in HTML format on your PC.

The device logs the following user actions, among others:

- A user logging on via CLI (local or remote)
- A user logging off manually
- Automatic logging off of a user in CLI after a specified period of inactivity
- Device restart
- Locking of a user account due to too many failed logon attempts
- Locking of the management access due to failed logon attempts
- Commands executed in CLI, apart from show commands
- Changes to configuration variables
- Changes to the system time
- File transfer operations, including firmware updates
- Configuration changes via HiDiscovery
- Firmware updates and automatic configuration of the device via the external memory
- Opening and closing of SNMP via an HTTPS tunnel

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Search	Opens the "Search" dialog. The dialog allows you to search the log file for search terms or regular expressions.
Save	Opens the "Save" dialog. The dialog allows you to save the log file in HTML format on your PC.
Help	Opens the online help.

Table 186: Buttons

8.2 Ports

This menu shows information on the port statistics, and on the connected SFP transceivers.

The menu contains the following dialogs:

- Statistics Table
- SFP

8.2.1 Statistics Table

This dialog shows you in table form for each device port how many data packets the device has sent and received.
To reset the values in the table to 0, click Reset port counters in the "Basic Settings:Restart" dialog.

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 187:Buttons

8.2.2 SFP

This dialog allows you to look at the SFP transceivers currently connected to the device and their properties.

■ Table

The table only displays valid values if the device is equipped with SFP transceivers.

Parameters	Meaning
Port	Device port to which the table entry relates.
Module Type	Type of the SFP transceiver, e.g. M-SFP-SX/LC.
Serial Number	Serial number of the SFP module.
Supported	Shows whether the media module supports the SFP transceiver.
Temperature in °Celsius	Operating temperature of the SFP transceiver in °Celsius.
Tx Power in mW	Transmission power of the SFP transceiver in mW.
Rx Power in mW	Receiving power of the SFP transceiver in mW.
Tx Power in dBm	Transmission power of the SFP transceiver in dBm.
Rx Power in dBm	Receiving power of the SFP transceiver in dBm.
Rx Power State	Power level of the signal received: The threshold values are specified by the SFP transceiver. ✓ Signal strength is OK. ⚠ Signal strength is lower than the SFP manufacturer recommendation. The signal can still be used. ✗ No signal or signal strength too low.

Table 188:"SFP" dialog, table

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 189:Buttons

8.3 Configuration Check

The device enables you to compare the device configuration with those of its neighboring devices. For this purpose, the device uses the information that it received from its neighboring devices via topology recognition (LLDP).

The dialog lists the deviations detected, which affect the performance of the communication between the device and the recognized neighboring devices.

You update the content of the table via the "Load" button. If the table remains empty, the configuration check was successful and the device configuration is compatible with the device configuration in the detected neighboring devices.

Summary

Parameters	Meaning
Number of Errors	Shows the number of errors that the device detected during the configuration check.
Number of Warnings	Shows the number of warnings that the device detected during the configuration check.
Amount of Information	Shows the amount of information that the device detected during the configuration check.

Table 190:"Configuration Check" dialog, "Summary" frame

You will also find this information in the tool bar above the menu. See “Operating Instructions” on page 14.

Table

When you select a row in the table, the device displays additional information in the area beneath it.

Parameters	Meaning
Rule ID	Rule ID of the deviations having occurred. The dialog combines several deviations with the same rule ID under one rule ID.
Level	Level of deviation between this device's configuration and the recognized neighboring devices. The rule level can have 3 statuses: ℹ Information: The performance of the communication between the two devices is not impaired. ⚠ Warning: The performance of the communication between the two devices may be impaired. ✖ Error: Communication between the two devices is impaired.
Message	The dialog specifies more precisely the information, warnings and errors having occurred.

Table 191:"Configuration Check" dialog, table

Note: The dialog shows the devices detected as connected to the neighboring device as if they were directly connected to the device itself.

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 192:Buttons

8.4 ARP

The device allows you to display the MAC address and the IP address of the devices connected to its device ports. The device uses the Address Resolution Protocol (ARP) for this.

■ Table

Parameters	Meaning
Port	Number or name of the port to which the table entry relates.
MAC Address	Shows the MAC address of a device that responded to an ARP query to this device port.
IP Address	Shows the IP address of a device that responded to an ARP query to this device port.
Type	Displays the type of the address entry. Possible values: ▶ `static` Static ARP entry. This entry is kept when the ARP table is deleted. ▶ `dynamic` Dynamic entry. The device deletes this entry when the “Aging Time” has been exceeded, if the device does not receive any data from this device during this time. ▶ `local` IP and MAC address of the device’s own device port.

Table 193:"ARP" dialog, table

To reset the counters, click `Reset ARP table` in the "Basic Settings:Restart" dialog.
See “Restart” on page 44.

Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 194: Buttons

8.5 Device Status

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device in order to present its condition in graphic form.

The device displays its current status as "Error" or "OK" in the "Device Status" frame. The device determines this status from the individual monitoring results.

Device Status

Parameters	Meaning
Device Status	Displays the current status of the device. The device determines the status from the individual monitored parameters. Possible values: ▶ `Error` ▶ `OK`

Table 195: "Device Status" dialog, "Device Status" frame

Trap Configuration

Parameters	Meaning
Generate Trap	Activates/deactivates the sending of an SNMP message (trap) when the value in the "Device Status" field changes. Possible values: ▶ `Selected` The device sends a trap. ▶ `Not selected` (default setting) The device does not send a trap. The prerequisite for sending SNMP messages (traps) is that the function is switched on in the `Diagnostics:Alarms (Traps)` dialog and at least 1 SNMP manager is defined.

Table 196: "Device Status" dialog, "Trap Configuration" frame

■ Monitoring

Parameters	Meaning
Temperature	Defines whether the device monitors the temperature in the device. Possible values: ▶ `Ignore` The device ignores this parameter. ▶ `Monitor` (default setting) The device changes the device status to `Error` if the temperature exceeds or falls below the temperature thresholds. You define the temperature thresholds in the `Basic Settings:System` dialog, in the "Temperature (°C)" field.
Connection error	Defines whether the device monitors the link status of the device ports. Possible values: ▶ `Ignore` (default setting) The device ignores this parameter. ▶ `Monitor` The device changes the device status to `Error` if the link at a device port is interrupted. You have the option of selecting the device ports to be monitored individually.
ENVM removal	Defines whether the device monitors the active external memory. Possible values: ▶ `Ignore` (default setting) The device ignores this parameter. ▶ `Monitor` The device changes the device status to `Error` if you remove the active external memory from the device. You specify the active external memory in the `Basic Settings:Load/Save` dialog, "External Memory" frame.
ENVM not in Sync	Defines whether the device monitors the synchronization of the device configuration in the device and on the external memory. Possible values: ▶ `Ignore` (default setting) The device ignores this parameter. ▶ `Monitor` The device changes the device status to `Error` in the following situations: – The device configuration only exists in the device. – The device configuration in the device differs from the device configuration on the external memory.

Table 197: "Device Status" dialog, "Monitoring" frame

■ “Port/Propagate Connection Error” table

Parameters	Meaning
Port	Device port to which the table entry relates.
Propagate Connection Error	Defines whether the device monitors the link status of the port. Possible values: ▶ `Selected` The device changes the device status to `Error` if the link at this port is interrupted. ▶ `Not selected` (default setting) The device status remains unchanged if the link at this port is interrupted. This setting is only effective if you have selected the value "Monitor" in the `Connection error` field, see "Monitoring" frame.

Table 198:"Device Status" dialog, “Port/Propagate Connection Error” table

■ “Power Supply/Propagate State” table

Parameters	Meaning
Power Supply	Number of the power supply that applies to this entry.
Propagate State	Defines whether the device monitors the power supply. Possible values: ▶ `Selected` (default setting) The device changes the device status to `Error` if one of the following conditions applies: – The voltage source is providing an incorrect voltage. – The voltage source fails. – The power supply within the device is defective. ▶ `Not selected` The device status remains unchanged under the conditions named above.

Table 199:"Device Status" dialog, “Power Supply/Propagate State” table

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 200: Buttons

8.6 Signal Contact

The signal contact is a potential-free relay contact. The device thus allows you to perform remote diagnosis. The device uses the relay contact to signal the occurrence of events by opening the relay contact and interrupting the closed circuit.

In this dialog you define the trigger conditions for the signal contact.

The signal contact gives you the following options:

- Monitoring the correct operation of the device.
- Signaling the device status of the device.
- Signaling the security status of the device.
- Controlling external devices by manually setting the signal contacts.

Signal Contact Mode

Parameters	Meaning
Signal Contact Mode	Specifies which events the device signals via the signal contact. Possible values: ▶ `Monitoring Correct Operation` (default setting) In this mode the signal contact signals events that occur when monitoring individual device functions. The signal contact thus makes remote diagnosis possible. In the "Monitoring Correct Operation" frame, you define additional settings. ▶ `Manual Setting` With this mode you can control the signal contact remotely. In the "Manual Setting" frame, you define additional settings. ▶ `Device Status` In this mode the signal contact signals the overall status from the "Device Status" dialog. The "Status" frame shows the status.

Table 201:"Signal Contact" dialog, “Signal Contact Mode” frame

■ Trap Configuration

Parameters	Meaning
Generate Trap	Activates/deactivates the sending of an SNMP message (trap) when an event occurs that triggers the signal contact. Possible values: ▶ `Selected` The device sends a trap. ▶ `Not selected` (default setting) The device does not send a trap. The prerequisite for sending SNMP messages (traps) is that the function is switched on in the `Diagnostics:Alarms (Traps)` dialog and at least 1 SNMP manager is defined.

Table 202:"Signal Contact" dialog, "Trap Configuration" frame

Function Monitoring

In this frame you define the parameters that the device monitors. The device signals the occurrence of an event by opening the signal contact.

Parameters	Meaning
Contact	Shows the status of the signal contact. Possible values: ▶ `Opened (Error)` An event has occurred that triggers the signal contact. The signal contact is opened. ▶ `Closed (OK)` Normal status. The signal contact is closed.
Temperature	Defines whether the signal contact monitors the temperature in the device. Possible values: ▶ `Ignore` The signal contact ignores this parameter. ▶ `Monitor` (default setting) The signal contact opens if the temperature exceeds / falls below the threshold values. You define the temperature thresholds in the `Basic Settings:System` dialog, in the "Temperature (°C)" field.
Connection error	Defines whether the signal contact monitors the link status of the device ports. Possible values: ▶ `Ignore` (default setting) The signal contact ignores this parameter. ▶ `Monitor` The signal contact opens if the link on a device port is interrupted. You have the option of selecting the device ports to be monitored individually.
ENVM removal	Defines whether the signal contact monitors the external memory. Possible values: ▶ `Ignore` (default setting) The signal contact ignores this parameter. ▶ `Monitor` The signal contact opens if you remove the external memory from the device.

Table 203:"Signal Contact" dialog, "Monitoring Correct Operation" frame

Parameters	Meaning
ENVM not in Sync	Defines whether the signal contact monitors the synchronization of the device configuration in the device and on the external memory. Possible values: ▶ `Ignore` (default setting) The signal contact ignores this parameter. ▶ `Monitor` The signal contact opens in the following situations. – The device configuration only exists in the device. – The device configuration in the device differs from the device configuration on the external memory.

Table 203:"Signal Contact" dialog, "Monitoring Correct Operation" frame (Cont.)

■ Manual Setting

This frame allows you to control the signal contact remotely. This is useful in the following situations, for example:

- Simulating an error during SPS error monitoring.
- Remote control of a device via SNMP, such as switching on a camera.

Parameters	Meaning
Contact	Defines the status of the signal contact. Possible values: ▶ `Opened` (default value) The signal contact is opened. ▶ `Closed` The signal contact is closed.

Table 204:"Signal Contact" dialog, "Manual Setting" frame

■ Status

This frame shows the status of the signal contact:

- The signal contact indicates the device status if you have selected the "Device Status" option field in the "Signal Contact Mode" frame.

Parameters	Meaning
Contact	Shows the status of the signal contact. The signal contact indicates the device status. Possible values: ▶ `Opened (Error)` The signal contact is opened. – The current status of the device has the value `Error`. or – The current status of the security-relevant settings in the device has the value `Error`. ▶ `Closed (OK)` Normal status. The signal contact is closed.

Table 205:"Signal Contact" dialog, "Status" frame

■ “Port/Propagate Connection Error” table

Parameters	Meaning
Port	Device port to which the table entry relates.
Propagate Connection Error	Defines whether the signal contact monitors the link status of the device port. Possible values: ▶ `Selected` (default setting) The signal contact opens if the link on this device port is interrupted. ▶ `Not selected` The signal contact remains closed if the link on this device port is interrupted. This setting is only effective if you have selected the value "Monitor" in the `Connection error` field, see "Function Monitoring" frame.

Table 206:"Signal Contact" dialog, “Port/Propagate Connection Error” table

“Power Supply/Propagate State” table

Parameters	Meaning
Port	Device port to which the table entry relates.
Propagate State	Defines whether the signal contact monitors the power supply. Possible values: ▶ Selected The signal contact opens if one of the following conditions applies: – The voltage source is providing an incorrect voltage. – The voltage source fails. – The power supply within the device is defective. ▶ Not selected (default setting) The signal contact remains closed under the conditions named above.

Table 207:"Signal Contact" dialog, “Power Supply/Propagate State” table

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Help	Opens the online help.

Table 208:Buttons

8.7 Alarms (Traps)

The device enables you to send an SNMP message (trap) yourself for specific events to one or more SNMP managers.
You define the events, for example, in the `Diagnostics:Device Status` dialog.

With this dialog you can define the SNMP managers to which the device sends the traps.

■ Operation

Parameters	Meaning
Operation	When the function is switched on, the device sends SNMP messages (traps) to the SNMP managers defined in the table. When the function is switched off, the device does not send any traps. Possible values: ▶ `On` (default setting) ▶ `Off`

Table 209:"Alarms (Traps)" dialog, "Operation" frame

Table

Parameters	Meaning
Name	Defines a name for the SNMP manager. Possible values: ▶ 1..32 alphanumeric characters ▶ including the following special characters: !#$%&'()*+,-./:;<=>?@[\\]^_`{}~
Address	Defines the IP address and the port number of the SNMP manager. Possible values: ▶ `<Valid IPv4 address>:<port number>`
Active	Defines whether the device sends SNMP messages (traps) to this SNMP manager. Possible values: ▶ `Selected` The device sends traps to this SNMP manager. ▶ `Not selected` The device does not send traps to this SNMP manager.

Table 210: "Alarms (Traps)" dialog, table

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Opens the "Create" dialog to add a new entry to the table. In the "Create" dialog you define the name and the IP address and port number of the SNMP manager. If you choose not to enter a port number, the device automatically adds the port number `162`.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 211: Buttons

8.8 Selftest

This dialog allows you to do the following:

- Enable/disable the switch to the system monitor when the device is being started.
- Defines how the device behaves in the case of an error.

Configuration

Parameters	Meaning
Activate SysMon1	Activates/deactivates the access to the system monitor during the restart. Possible values: ▶ `Selected` (default setting) The device allows you to switch to the system monitor during the restart. ▶ `Not selected` The device starts without the option to switch to the system monitor. Among other things, the system monitor allows you to update the device software or delete saved device configurations.
Load default config on error	Activates/deactivates the loading of the standard device configuration (`default configuration`) if no readable device configuration is available for the device when it is restarting. Possible values: ▶ `Selected` (default setting) The device loads the standard device configuration. ▶ `Not selected` The device interrupts the restart and stops. To get access to the device again, use a V.24 link to switch to the system monitor and load the standard device configuration there.

Table 212: "Selftest" dialog, "Configuration" frame

Note: The following settings block your access to the device permanently if no readable device configuration is available for the device when it is restarting. This is the case, for example, if the password for the device configuration to be loaded differs from the password set in the device.

- "Activate SysMon1" checkbox is `not selected`.
- "Load default config on error" checkbox is `not selected`.

To have the device unlocked again, contact your sales partner.

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 213: Buttons

9 Advanced

With this menu you can configure additional settings for the device.

The menu contains the following dialogs:

- DNS

9.1 DNS

DNS (Domain Name System) is a service in the network that translates host names into IP addresses. This name resolution gives you the option of contacting other devices using their host names instead of their IP addresses.

The integrated DNS-client function enables the device to send requests for name resolutions to one or more DNS servers.

If the DNS cache is activated, the device saves the responses of the DNS servers in the memory. If the device is operating as a DNS server in the internal network , it responds to repeated requests itself without contacting the DNS server again. The device sends new requests to the DNS server(s) in the usual manner.

The menu contains the following dialogs:

- Global
- Server
- Cache

9.1.1 Global

This dialog gives you the option of the DNS-client function in the device on or off.

■ Operation

Parameter	Meaning
Operation	If the function is switched on, the device sends requests for name resolution to the specified DNS servers. Possible values: ▶ `On` DNS-client function is switched on. ▶ `Off` (default setting) DNS-client function is switched off.

Table 214:"DNS Global"dialog, "Operation" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 215:Buttons

9.1.2 Server

In this menu you see the DNS servers currently being used. In addition you have the possibility of specifying where the device obtains the IP addresses of the DNS servers to which the requests are to be addressed.

This menu contains the following dialogs:

- Current
- Static

9.1.3 Current

This dialog displays the DNS servers to which the device sends requests for address resolution. Prerequisite for this is that the DNS-client function is enabled in the `Advanced:DNS:Global` dialog.

■ Table

Parameter	Meaning
Index	Shows a sequential number to which the table entry relates. The device automatically defines this number.
Address	Displays the IP address of the DNS server.

Table 216: "DNS Servers Current" dialog, table

■ Buttons

Button	Meaning
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Help	Opens the online help.

Table 217: Buttons

9.1.4 Static

In this menu you specify where the device obtains the IP addresses of the DNS servers to which the requests are to be addressed. In addition you have the possibility of adding IP addresses of DNS servers yourself.

■ Configuration

Parameter	Meaning
Configuration source	Specifies where the device obtains the IP addresses of DNS servers to which requests are to be addressed. Possible values: ▶ `user` (default setting) The device uses the DNS servers specified in the table. ▶ `provider` The device obtains the IP addresses of the DNS servers when dialing in from the service provider via a WAN connection. ▶ `mgmt-dhcp` The device obtains the IP addresses of the DNS servers from the DHCP server in the management VLAN.

Table 218:"DNS Servers Static" dialog, "Configuration" frame

Table

Parameter	Meaning
Index	Shows a sequential number to which the table entry relates. The device automatically defines this number. Possible values: ▶ `1..4`
Address	Specifies the IP address of the DNS server. Possible values: ▶ Valid IPv4 address (default setting`0.0.0.0`)
Active	Activates/deactivates the table entry. Possible values: ▶ `not selected` (default setting) The device does not send requests to this DNS server. ▶ `selected` The device sends requests to this DNS server if the following prerequisites are fulfilled: – Prerequisite for this is that the DNS-client function is enabled in the `Advanced:DNS:Global` dialog. – The value `user` is selected in the "Configuration Source" field in the "Configuration" frame. – The table entry has the smallest index or the device receives no response from the DNS server in the table entry with a smaller index.

Table 219:"DNS Servers Static" dialog, table

Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (`RAM`) of the device. To permanently save the changes, then choose the active device configuration in the `Basic Settings:Load/Save` dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (`RAM`) of the device.
Create	Adds a new table entry.
Remove	Removes the selected table entry.
Help	Opens the online help.

Table 220:Buttons

9.1.5 Cache

This dialog provides you with the possibility of activating or deactivating the DNS cache in the device.

■ Function

Button	Meaning
Operation	When the function is switched on, the DNS cache is activated in the device. Possible values: ▶ On (default setting) DNS cache is active. The device forwards requests to the DNS server and saves the responses in the memory. Repeated requests are answered by the device itself without contacting the DNS server again. The device functions as a DNS server in the internal network and reduces the load on the actual DNS server. ▶ Off DNS cache is disabled. The device always forwards requests to the DNS server without saving the responses in the memory.

Table 221:"DNS-Cache" dialog, "Operation" frame

■ Buttons

Button	Meaning
Set	Transfers the changes to the volatile memory (RAM) of the device. To permanently save the changes, then choose the active device configuration in the Basic Settings:Load/Save dialog and click "Save".
Reload	Updates the fields with the values that are saved in the volatile memory (RAM) of the device.
Clear DNS cache	Deletes the responses of the DNS server in the DNS cache.
Help	Opens the online help.

Table 222:Buttons

A Appendix

A.1 Technical Data

Switching	
Size of MAC address table (incl. static filters)	16384 (16k)
Max. number of statically configured MAC address filters	100
Max. length of over-long packets	1522 Bytes
Latency (with 64 Byte data packets)	
1.000 Mbit/s	Layer 2: typ. 3.3 µs
100 Mbit/s	Layer 2: typ. 8.3 µs
10 Mbit/s	Layer 2: typ. 50 µs
Number of Switch queues	8 queues
Port priorities that can be set	0..7

VLAN	
VLAN-ID	1..4042
Number of VLANs	max. 64 simultaneously per device max. 64 simultaneously per port

Routing/Switching	
Maximum number of additional IP addresses	64
Maximum number of static routing entries	256
Maximum number of VLAN Routing interfaces	64

Firewall	
Maximum number of L3 firewall rules	2048

NAT	
Maximum number of 1:1 NAT rules	255
Maximum number of Destination NAT rules	255
Maximum number of Double NAT rules	255
Maximum number of Masquerading NAT rules	128
Maximum number of Connection Tracking entries	7768

A.2 List of RFCs

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 951	BOOTP
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1191	Path MTU Discovery
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1812	Requirements for IP Version 4 Routers
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475	An Architecture for Differentiated Service
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2644	Changing the Default for Directed Broadcasts in Routers
RFC 2663	IP Network Address Translator (NAT) Terminology and Considerations
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB

RFC 2863	The Interfaces Group MIB
RFC 2865	RADIUS Client
RFC 3022	Traditional IP Network Address Translator
RFC 3164	The BSD Syslog Protocol
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4188	Definitions of Managed Objects for Bridges
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4318	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 5905	NTPv4

A.3 Underlying IEEE Standards

IEEE 802.1AB	Topology Discovery (LLDP)
IEEE 802.1D-2004	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering)
IEEE 802.1Q-2005	Virtual Bridged Local Area Networks (VLAN Tagging, Port Based VLANs)
IEEE 802.3-2002	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control

A.4 Maintenance

Hirschmann is continually working to improve and develop our software. You should regularly check whether there is a new version of the software that provides you with additional benefits. You will find software information and downloads on the product pages of the Hirschmann website.

A.5 Literature references

- „Optische Übertragungstechnik
  in industrieller Praxis“
  Christoph Wrobel (Hrsg.)
  Hüthig Buch Verlag Heidelberg
  ISBN 3-7785-2262-0

- Hirschmann Manual
  “Basics of Industrial ETHERNET and TCP/IP”
  280 710-834

- “TCP/IP Illustrated”, Vol. 1
  W.R. Stevens
  Addison Wesley 1994
  ISBN 0-201-63346-9

- Hirschmann “Installation” user manual

- Hirschmann “Basic Configuration” user manual

- Hirschmann “GUI Graphical User Interface” reference manual

- Hirschmann “Command Line Interface” reference guide

- Hirschmann Manual „Network Management System Industrial HiVision“

A.6 Copyright of Integrated Software

A.6.1 Network Time Protocol Version 4 Distribution

The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

- Mark Andrews <mark_andrews@isc.org> Leitch atomic clock controller
- Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices
- Viraj Bais <vbais@mailman1.intel.com> and Clayton Kirkwood <kirkwood@striderfm.intel.com> port to Windows NT 3.5
- Michael Barone <michael,barone@lmco.com> GPSVME fixes
- Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca>, IPv6 support
- Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
- Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.
- Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
- Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
- Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)

- Steve Clift <clift@ml.csiro.au> OMEGA clock driver
- Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
- Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
- John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
- Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
- Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
- John Hay <jhay@@icomtek.csir.co.za> IPv6 support and testing
- Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
- Mike Iglesias <iglesias@uci.edu> DEC Alpha port
- Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
- Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
- Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or <H.Lambermont@chello.nl> ntpsweep
- Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
- Frank Kardel <kardel (at) ntp (dot) org> PARSE <GENERIC> driver (>14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
- William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
- Dave Katz <dkatz@cisco.com> RS/6000 AIX port
- Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
- George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
- Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
- Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
- Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance
- David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
- Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
- Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
- Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
- Kamal A Mostafa <kamal@whence.com> SCO OpenServer port

- Derek Mulcahy <derek@toybox.demon.co.uk> and Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
- Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
- Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
- Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo
- Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
- Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
- Ray Schnitzler <schnitz@unipress.com> Unixware1 port
- Michael Shields <shields@tembel.org> USNO clock driver
- Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
- Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
- Kenneth Stone <ken@sdd.hp.com> HP-UX port
- Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support
- Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
- Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
- Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

B Index

C Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very Good	**Good**	**Satisfactory**	**Mediocre**	**Poor**
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127/14-1600 or
- per mail to

Hirschmann Automation and Control GmbH
Department 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen

D Further Support

Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at http://www.hirschmann.com

Contact our support at https://hirschmann-support.belden.eu.com

You can contact us

in the EMEA region at
- Tel.: +49 (0)1805 14-1538
- E-mail: hac.support@belden.com

in the America region at
- Tel.: +1 (717) 217-2270
- E-mail: inet-support.us@belden.com

in the Asia-Pacific region at
- Tel.: +65 6854 9860
- E-mail: inet-ap@belden.com

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  The current technology and product training courses can be found at http://www.hicomcenter.com
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND